SIEMENS

RUGGEDCOM ROS v4.1

User Guide

For RMC30

12/2014
RC1105-EN-02

Preface

Introduction 1

Using ROS 2

Device Management 3

System Administration 4

Setup and Configuration 5

Troubleshooting 6

Copyright © 2014 Siemens Canada Ltd.

All rights reserved. Dissemination or reproduction of this document, or evaluation and communication of its contents, is not authorized except where expressly permitted. Violations are liable for damages. All rights reserved, particularly for the purposes of patent application or trademark registration.

This document contains proprietary information, which is protected by copyright. All rights are reserved. No part of this document may be photocopied, reproduced or translated to another language without the prior written consent of Siemens Canada Ltd..

Disclaimer Of Liability

Siemens has verified the contents of this manual against the hardware and/or software described. However, deviations between the product and the documentation may exist.

Siemens shall not be liable for any errors or omissions contained herein or for consequential damages in connection with the furnishing, performance, or use of this material.

The information given in this document is reviewed regularly and any necessary corrections will be included in subsequent editions. We appreciate any suggested improvements. We reserve the right to make technical improvements without notice.

Registered Trademarks

ROX™, Rugged Operating System On Linux™, CrossBow™ and ELAN™ are trademarks of Siemens Canada Ltd. . ROS® is a registered trademark of Siemens Canada Ltd..

Other designations in this manual might be trademarks whose use by third parties for their own purposes would infringe the rights of the owner.

Third Party Copyrights

Siemens recognizes the following third party copyrights:

- Copyright © 2004 GoAhead Software, Inc. All Rights Reserved.

Security Information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, machines, equipment and/or networks. They are important components in a holistic industrial security concept. With this in mind, Siemens ' products and solutions undergo continuous development. Siemens recommends strongly that you regularly check for product updates.

For the secure operation of Siemens products and solutions, it is necessary to take suitable preventive action (e.g. cell protection concept) and integrate each component into a holistic, state-of-the-art industrial security concept. Third-party products that may be in use should also be considered. For more information about industrial security, visit http://www.siemens.com/industrialsecurity.

To stay informed about product updates as they occur, sign up for a product-specific newsletter. For more information, visit http://support.automation.siemens.com.

Warranty

Refer to the License Agreement for the applicable warranty terms and conditions, if any.

For warranty details, visit www.siemens.com/ruggedcom or contact a Siemens customer service representative.

Contacting Siemens

Address

Siemens Canada Ltd.
Industry Sector
300 Applewood Crescent
Concord, Ontario
Canada, L4K 5C7

Telephone

Toll-free: 1 888 264 0006
Tel: +1 905 856 5288
Fax: +1 905 856 1995

E-mail

ruggedcom.info.i-ia@siemens.com

Web

www.siemens.com/ruggedcom

Table of Contents

Preface ix
Conventions ix
Alerts ix
CLI Command Syntax x
Related Documents x
System Requirements x
Accessing Documentation xi
Training xi
Customer Support xi

Chapter 1
Introduction 1
1.1 Overview 1
1.2 Security Recommendations and Considerations 2
1.2.1 Security Recommendations 2
1.2.2 Key Files 3
1.2.2.1 SSL Certificates 4
1.2.2.2 SSH Key Pairs 5
1.3 Available Services by Port 6
1.4 SNMP Management Interface Base (MIB) Support 9
1.4.1 Supported Standard MIBs 9
1.4.2 Supported Proprietary RUGGEDCOM MIBs 10
1.4.3 Supported Agent Capabilities 10
1.5 SNMP Traps 11
1.6 ModBus Management Support 12
1.6.1 ModBus Function Codes 13
1.6.2 ModBus Memory Map 14
1.6.3 ModBus Memory Formats 19
1.6.3.1 Text 19
1.6.3.2 Cmd 19
1.6.3.3 Uint16 20
1.6.3.4 Uint32 20
1.6.3.5 PortCmd 20
1.6.3.6 Alarm 21
1.6.3.7 PSStatusCmd 21

1.6.3.8 TruthValues 22
1.7 Certificate and Key Requirements 22

Chapter 2
Using ROS 25
2.1 Connecting to ROS 25
2.1.1 Connecting Directly 25
2.1.2 Connecting via the Network 26
2.2 Logging In 27
2.3 Logging Out 28
2.4 Using the Web Interface 28
2.5 Using the Console Interface 30
2.6 Using the Command Line Interface 32
2.6.1 Available CLI Commands 32
2.6.2 Tracing Events 35
2.6.3 Executing Commands Remotely via RSH 36
2.6.4 Using SQL Commands 36
2.6.4.1 Finding the Correct Table 37
2.6.4.2 Retrieving Information 37
2.6.4.3 Changing Values in a Table 39
2.6.4.4 Resetting a Table 39
2.6.4.5 Using RSH and SQL 39
2.7 Selecting Ports in ROS 40
2.8 Managing the Flash File System 40
2.8.1 Viewing a List of Flash Files 40
2.8.2 Viewing Flash File Details 41
2.8.3 Defragmenting the Flash File System 42
2.9 Accessing BIST Mode 42

Chapter 3
Device Management 43
3.1 Viewing Product Information 43
3.2 Viewing CPU Diagnostics 45
3.3 Restoring Factory Defaults 46
3.4 Configuring an IP Interface 47
3.5 Uploading/Downloading Files 47
3.5.1 Uploading/Downloading Files Using XMODEM 48
3.5.2 Uploading/Downloading Files Using a TFTP Client 49
3.5.3 Uploading/Downloading Files Using a TFTP Server 50
3.5.4 Uploading/Downloading Files Using an SFTP Server 50
3.6 Managing Logs 51

3.6.1 Viewing Local Logs 51
3.6.2 Clearing Local Logs 52
3.6.3 Configuring the Local System Log 52
3.6.4 Managing Remote Logging 53
3.6.4.1 Configuring the Remote Syslog Client 53
3.6.4.2 Viewing a List of Remote Syslog Servers 54
3.6.4.3 Adding a Remote Syslog Server 54
3.6.4.4 Deleting a Remote Syslog Server 56
3.7 Managing IP Gateways 57
3.7.1 Viewing a List of IP Gateways 57
3.7.2 Adding an IP Gateway 57
3.7.3 Deleting an IP Gateway 59
3.8 Configuring IP Services 59
3.9 Managing Remote Monitoring 61
3.9.1 Managing RMON History Controls 61
3.9.1.1 Viewing a List of RMON History Controls 61
3.9.1.2 Adding an RMON History Control 62
3.9.1.3 Deleting an RMON History Control 63
3.9.2 Managing RMON Alarms 64
3.9.2.1 Viewing a List of RMON Alarms 65
3.9.2.2 Adding an RMON Alarm 66
3.9.2.3 Deleting an RMON Alarm 68
3.9.3 Managing RMON Events 69
3.9.3.1 Viewing a List of RMON Events 70
3.9.3.2 Adding an RMON Event 70
3.9.3.3 Deleting an RMON Event 72
3.10 Upgrading/Downgrading Firmware 72
3.10.1 Upgrading Firmware 73
3.10.2 Downgrading Firmware 73
3.11 Resetting the Device 74
3.12 Decommissioning the Device 75

Chapter 4
System Administration 77
4.1 Configuring the System Information 77
4.2 Customizing the Login Screen 78
4.3 Configuring Passwords 78
4.4 Managing Alarms 81
4.4.1 Viewing a List of Pre-Configured Alarms 81
4.4.2 Viewing and Clearing Latched Alarms 82
4.4.3 Configuring an Alarm 83

4.4.4 Authentication Related Security Alarms 86
4.4.4.1 Security Alarms for Login Authentication 86
4.4.4.2 Security Messages for Port Authentication 88
4.5 Managing the Configuration File 89
4.5.1 Configuring Data Encryption 89
4.5.2 Updating the Configuration File 90
4.6 Managing an Authentication Server 91
4.6.1 Managing RADIUS Authentication 91
4.6.1.1 Configuring the RADIUS Server 92
4.6.1.2 Configuring the RADIUS Client 92
4.6.2 Managing TACACS+ Authentication 94
4.6.2.1 Configuring TACACS+ 94
4.6.2.2 Configuring User Priviliges 95

Chapter 5
Setup and Configuration 97
5.1 Managing Time Services 97
5.1.1 Configuring the Time and Date 97
5.1.2 Configuring NTP 98
5.2 Managing SNMP 100
5.2.1 Managing SNMP Users 100
5.2.1.1 Viewing a List of SNMP Users 101
5.2.1.2 Adding an SNMP User 101
5.2.1.3 Deleting an SNMP User 104
5.2.2 Managing Security-to-Group Mapping 105
5.2.2.1 Viewing a List of Security-to-Group Maps 105
5.2.2.2 Adding a Security-to-Group Map 105
5.2.2.3 Deleting a Security-to-Group Map 107
5.2.3 Managing SNMP Groups 107
5.2.3.1 Viewing a List of SNMP Groups 108
5.2.3.2 Adding an SNMP Group 108
5.2.3.3 Deleting an SNMP Group 110
5.3 Managing Network Discovery 110
5.4 Managing Serial Protocols 111
5.4.1 Encapsulation Concepts 113
5.4.1.1 Raw Socket Character Encapsulation 114
5.4.1.2 RTU Polling 114
5.4.1.3 Broadcast RTU Polling 115
5.4.1.4 Preemptive Raw Socket 116
5.4.1.5 Port Redirectors 117
5.4.1.6 Message Packetization 118

5.4.2 Modbus Concepts 118
5.4.2.1 Modbus Server Client Applications 118
5.4.2.2 Modbus TCP Performance Determinants 119
5.4.2.3 Turnaround Delay 121
5.4.3 DNP, Microlok, TIN and WIN Concepts 121
5.4.3.1 DNP, Microlok, TIN and WIN Applications 121
5.4.3.2 The Concept of Links 122
5.4.3.3 Address Learning for TIN 122
5.4.3.4 Address Learning for DNP 123
5.4.3.5 Broadcast Messages 124
5.4.3.6 Transport Protocols 124
5.4.4 Force Half-Duplex (HD) Operation Mode 125
5.4.5 Configuring a Serial Port 126
5.4.6 Configuring the Raw Socket Protocol 129
5.4.7 Configuring the Preemptive Raw Socket Protocol 131
5.4.8 Configuring a TCP Modbus Server 133
5.4.9 Configuring a TCP Modbus Client 134
5.4.10 Configuring the WIN and TIN Protocols 135
5.4.11 Configuring the MicroLok Protocol 137
5.4.12 Configuring the DNP Protocol 138
5.4.13 Configuring the DNP Over Raw Socket Protocol 140
5.4.14 Configuring the Mirrored Bits Protocol 141
5.4.15 Configuring the Telnet Com Port Protocol 143
5.4.16 Managing Raw Socket Remote Hosts 145
5.4.16.1 Viewing a List of Remote Hosts 145
5.4.16.2 Adding a Remote Host 146
5.4.16.3 Deleting a Remote Host 147
5.4.17 Managing Device Addresses 148
5.4.17.1 Viewing a List of Device Addresses 148
5.4.17.2 Adding a Device Address 149
5.4.17.3 Deleting a Device Address 150
5.4.18 Viewing the TIN Dynamic Address Table 151
5.4.19 Viewing Statistics for Serial Protocol Links 152
5.4.20 Viewing Statistics for Serial Protocol Connections 153
5.4.21 Viewing Serial Port Statistics 154
5.4.22 Clearing Statistics for Specific Serial Ports 155
5.4.23 Resetting Serial Ports 155

Chapter 6
Troubleshooting 157
6.1 General 157

Preface

This guide describes v4.1 of ROS (Rugged Operating System) running on the RUGGEDCOM RMC30. It contains instructions and guidelines on how to use the software, as well as some general theory.

It is intended for use by network technical support personnel who are familiar with the operation of networks. It is also recommended for us by network and system planners, system programmers, and line technicians.

IMPORTANT!
Some of the parameters and options described may not be available depending on variations in the device hardware. While every attempt is made to accurately describe the specific parameters and options available, this Guide should be used as a companion to the Help text included in the software.

Conventions

This User Guide uses the following conventions to present information clearly and effectively.

Alerts

The following types of alerts are used when necessary to highlight important information.

DANGER!
DANGER alerts describe imminently hazardous situations that, if not avoided, will result in death or serious injury.

WARNING!
WARNING alerts describe hazardous situations that, if not avoided, may result in serious injury and/or equipment damage.

CAUTION!
CAUTION alerts describe hazardous situations that, if not avoided, may result in equipment damage.

IMPORTANT!
IMPORTANT alerts provide important information that should be known before performing a procedure or step, or using a feature.

NOTE
NOTE alerts provide additional information, such as facts, tips and details.

CLI Command Syntax

The syntax of commands used in a Command Line Interface (CLI) is described according to the following conventions:

Example	Description
command	Commands are in bold.
command parameter	Parameters are in plain text.
command parameter1 parameter2	Parameters are listed in the order they must be entered.
command parameter1 *parameter2*	Parameters in italics must be replaced with a user-defined value.
command [parameter1 | parameter2]	Alternative parameters are separated by a vertical bar (|). Square brackets indicate a required choice between two or more parameters.
command {parameter3 | parameter4}	Curly brackets indicate an optional parameter(s).
command parameter1 parameter2 {parameter3 | parameter4}	All commands and parameters are presented in the order they must be entered.

Related Documents

Other documents that may be of interest include:

- *RUGGEDCOM RMC30 Installation Guide*
- *RUGGEDCOM RMC30 Data Sheet*
- *RUGGEDCOM Fiber Guide*
- *RUGGEDCOM Wireless Guide*
- *White Paper: Rapid Spanning Tree in Industrial Networks*

System Requirements

Each workstation used to connect to the ROS interface must meet the following system requirements:

- Must have one of the following Web browsers installed:
  - Microsoft Internet Explorer 8.0 or higher
  - Mozilla Firefox
  - Google Chrome
  - Iceweasel/IceCat (Linux Only)
- Must have a working Ethernet interface compatible with at least one of the port types on the RUGGEDCOM device
- The ability to configure an IP address and netmask on the computer's Ethernet interface

Accessing Documentation

The latest Hardware Installation Guides and Software User Guides for most RUGGEDCOM products are available online at www.siemens.com/ruggedcom.

For any questions about the documentation or for assistance finding a specific document, contact a Siemens sales representative.

Training

Siemens offers a wide range of educational services ranging from in-house training of standard courses on networking, Ethernet switches and routers, to on-site customized courses tailored to the customer's needs, experience and application.

Siemens' Educational Services team thrives on providing our customers with the essential practical skills to make sure users have the right knowledge and expertise to understand the various technologies associated with critical communications network infrastructure technologies.

Siemens' unique mix of IT/Telecommunications expertise combined with domain knowledge in the utility, transportation and industrial markets, allows Siemens to provide training specific to the customer's application.

For more information about training services and course availability, visit www.siemens.com/ruggedcom or contact a Siemens sales representative.

Customer Support

Customer support is available 24 hours, 7 days a week for all Siemens customers. For technical support or general information, contact Siemens Customer Support through any of the following methods:

- **Online**

  Visit http://www.siemens.com/automation/support-request to submit a Support Request (SR) or check on the status of an existing SR.

- **Telephone**

  Call a local hotline center to submit a Support Request (SR). To locate a local hotline center, visit http://www.automation.siemens.com/mcms/aspa-db/en/automation-technology/Pages/default.aspx.

- **Mobile App**

  Install the Industry Online Support app by Siemens AG on any Android, Apple iOS or Windows mobile device and be able to:

  - Access Siemens' extensive library of support documentation, including FAQs, manuals, and much more
  - Submit SRs or check on the status of an existing SR
  - Find and contact a local contact person
  - Ask questions or share knowledge with fellow Siemens customers and the support community
  - And much more...

1 Introduction

This chapter provides a basic overview of the ROS software. It describes the following topics:

- Section 1.1, “Overview”
- Section 1.2, “Security Recommendations and Considerations”
- Section 1.3, “Available Services by Port”
- Section 1.4, “SNMP Management Interface Base (MIB) Support”
- Section 1.5, “SNMP Traps”
- Section 1.6, “ModBus Management Support”
- Section 1.7, “Certificate and Key Requirements”

Section 1.1

Overview

Welcome to the ROS Software User Guide for the RMC30. This Guide describes the wide array of carrier grade features made available by ROS (Rugged Operating System). These features include:

IMPORTANT!
The RMC30 is not intended for use or resale as online control equipment in hazardous, high-risk environments that require fail-safe performance, such as nuclear facilities, aircraft navigation or communication systems, air traffic control, direct life support machines or weapons systems, in which the failure of the software could result in death, personal injury, or severe physical or environmental damage.

Cyber Security Features

- Muti-level user passwords
- SSH/SSL (128-bit encryption)
- RADIUS centralized password management
- SNMPv3 authentication and 56-bit encryption

Management Features

- Web-based, Telnet, CLI management interfaces
- SNMP v1/v2/v3 (56-bit encryption)
- Remote Monitoring (RMON)
- Rich set of diagnostics with logging and alarms

Section 1.2

Security Recommendations and Considerations

The following describes important security-related recommendations and suggestions that should be considered before implementing the RMC30 on any network:

- Section 1.2.1, “Security Recommendations”
- Section 1.2.2, “Key Files”

Section 1.2.1

Security Recommendations

To prevent unauthorized access to the device, note the following security recommendations:

- Do not connect the device to the Internet. Deploy the device only within a secure network perimeter.
- Replace the default passwords for all user accounts and processes (where applicable) before the device is deployed.
- Use strong passwords. Avoid weak passwords such as *password1*, *123456789*, *abcdefgh*, etc. For more information about creating strong passwords, refer to the password requirements in Section 4.3, “Configuring Passwords”.
- Make sure passwords are protected and not shared with unauthorized personnel.
- Passwords should not be re-used across different usernames and systems, or after they expire.
- When RADIUS authentication is done remotely, make sure all communications are within the security perimeter or on a secure channel.
- SSL and SSH keys are accessible to users who connect to the device via the serial console. Make sure to take appropriate precautions when shipping the device beyond the boundaries of the trusted environment:
  - Replace the SSH and SSL keys with *throwaway* keys prior to shipping.
  - Take the existing SSH and SSL keys out of service. When the device returns, create and program new keys for the device.
- Restrict physical access to the device to only trusted personnel. A person with malicious intent could extract critical information, such as certificates, keys, etc. (user passwords are protected by hash codes), or reprogram the device.
- Control access to the serial console to the same degree as any physical access to the device. Access to the serial console allows for potential access to the ROS boot loader, which includes tools that may be used to gain complete access to the device.
- Only enable services that will be used on the device, including physical ports. Unused physical ports could potentially be used to gain access to the network behind the device.
- If SNMP is enabled, limit the number of IP addresses that can connect to the device and change the community names. Also configure SNMP to raise a trap upon authentication failures. For more information, refer to Section 5.2, “Managing SNMP”.
- Avoid using insecure services such as Telnet and TFTP, or disable them completely if possible. These services are available for historical reasons and are disabled by default.
- Limit the number of simultaneous Web Server, Telnet and SSH sessions allowed.
- Configure remote system logging to forward all logs to a central location. For more information, refer to Section 3.6, “Managing Logs”.

- Configuration files are provided in the CSV (comma separated values) format for ease of use. Make sure configuration files are properly protected when they exist outside of the device. For instance, encrypt the files, store them in a secure place, and do not transfer them via insecure communication channels.
- Management of the configuration file, certificates and keys is the responsibility of the device owner. Before returning the device to Siemens for repair, make sure encryption is disabled (to create a cleartext version of the configuration file) and replace the current certificates and keys with temporary *throwaway* certificates and keys that can be destroyed upon the device's return.
- Be aware of any non-secure protocols enabled on the device. While some protocols, such as HTTPS and SSH, are secure, others, such as Telnet and RSH, were not designed for this purpose. Appropriate safeguards against non-secure protocols should be taken to prevent unauthorized access to the device/network.
- Periodically audit the device to make sure it complies with these recommendations and/or any internal security policies.

Section 1.2.2
Key Files

ROS uses security keys to establish secure remote logins (SSH) and Web access (SSL).

It is strongly recommended that a unique SSL certificate and SSH keys be created and provisioned. New ROS - based units from Siemens will be shipped with a unique certificate and keys preconfigured in the `ssl.crt` and `ssh.keys` flash files.

The default and auto-generated SSL certificates are self-signed. It is recommended to use an SSL certificate that is either signed by a trusted third-party Certificate Authority (CA) or by an organization's own CA. This technique is described in the Siemens application note: *Creating/Uploading SSH Keys and SSL Certificates to ROS Using Windows*, available from www.siemens.com/ruggedcom.

The sequence of events related to Key Management during an upgrade to ROS v4.1 or later is as follows:

NOTE
The auto-generation of SSH keys is not available for Non-Controlled (NC) versions of ROS.

- On first boot, ROS will start the SSH and SSL services using the *default keys*.
- Immediately after boot, ROS will start to generate a unique SSL certificate and SSH key pair, and save each one to its corresponding flash file. As each one is created, the corresponding service is immediately restarted with the new keys.
- At any time during the key generation process, custom keys can be uploaded. The custom keys will take precedence over both the default and auto-generated keys.
- On subsequent boot, if there is a valid `ssl.crt` file, the default certificate will not be used for SSL. If there is a valid `ssh.keys` file, the default SSH key will not be used.
- At any time, new keys may be uploaded or generated by ROS using the `sslkeygen` or `sshkeygen` CLI commands.

The following sections describe SSL certificates and SSH key pairs in more detail:

- Section 1.2.2.1, “SSL Certificates”
- Section 1.2.2.2, “SSH Key Pairs”

Section 1.2.2.1
SSL Certificates

ROS supports SSL certificates that conform to the following specifications:

- X.509 v3 digital certificate format
- PEM format
- RSA key pair, 512 to 2048 bits

The RSA key pair used in the default certificate and in those generated by ROS uses a public key of 1024 bits in length.

NOTE
RSA keys smaller than 1024 bits in length are not recommended. Support is only included here for compatibility with legacy equipment.

NOTE
The default certificate and keys are common to all ROS versions without a certificate or key files. That is why it is important to either allow the key auto-generation to complete or to provision custom keys. In this way, one has at least unique, and at best, traceable and verifiable keys installed when establishing secure communication with the unit.

The following (bash) shell script fragment uses the `openssl` command line utility to generate a self-signed X.509 v3 SSL certificate with a 1024 bit RSA key suitable for use in ROS . Note that two standard PEM files are required: the SSL certificate and the RSA private key file. These are concatenated into the resulting `ssl.crt` file, which may then be uploaded to ROS:

```
# RSA key size:
BITS=1024
# 20 years validity:
DAYS=7305

# Values that will be stored in the Distinguished Name fields:

COUNTRY_NAME=CA                    # Two-letter country code
STATE_OR_PROVINCE_NAME=Ontario     # State or Province
LOCALITY_NAME=Concord              # City
ORGANIZATION=Ruggedcom.com         # Your organization's name
ORGANIZATION_CA=${ORGANIZATION}_CA # Your Certificate Authority
COMMON_NAME=RC                     # The DNS or IP address of the ROS unit
ORGANIZATIONAL_UNIT=ROS            # Organizational unit name

# Variables used in the construction of the certificate
REQ_SUBJ="/C=${COUNTRY_NAME}/ST=${STATE_OR_PROVINCE_NAME}/L=${LOCALITY_NAME}/O=${ORGANIZATION}/OU=
${ORGANIZATIONAL_UNIT}/CN=${COMMON_NAME}/"
REQ_SUBJ_CA="/C=${COUNTRY_NAME}/ST=${STATE_OR_PROVINCE_NAME}/L=${LOCALITY_NAME}/O=${ORGANIZATION_CA}/
OU=${ORGANIZATIONAL_UNIT}/"

#####################################################################
# Make the self-signed SSL certificate and RSA key pair:

openssl req -x509 -newkey rsa:${BITS} -nodes \
 -days ${DAYS} -subj ${REQ_SUBJ} \
 -keyout ros_ssl.key  \
 -out    ros_ssl.crt

# Concatenate Cert and Key into a single file suitable for upload to ROS:
# Note that cert must precede the RSA key:
cat  ros_ssl.crt  ros_ssl.key > ssl.crt
```

For information on creating SSL certificates for use with ROS in a Microsoft Windows environment, refer to the following Siemens application note: *Creating/Uploading SSH Keys and SSL Certificates to ROS Using Windows*.

The following is an example of a self-signed SSL certificate generated by ROS:

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            ca:01:2d:c0:bf:f9:fd:f2
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=CA, ST=Ontario, L=Concord, O=RuggedCom.com, OU=RC, CN=ROS
        Validity
            Not Before: Dec  6 00:00:00 2012 GMT
            Not After : Dec  7 00:00:00 2037 GMT
        Subject: C=CA, ST=Ontario, L=Concord, O=RuggedCom.com, OU=RC, CN=ROS
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:83:e8:1f:02:6b:cd:34:1f:01:6d:3e:b6:d3:45:
                    b0:18:0a:17:ae:3d:b0:e9:c6:f2:0c:af:b1:3e:e7:
                    fd:f2:0e:75:8d:6a:49:ce:47:1d:70:e1:6b:1b:e2:
                    fa:5a:1b:10:ea:cc:51:41:aa:4e:85:7c:01:ea:c3:
                    1e:9e:98:2a:a9:62:48:d5:27:1e:d3:18:cc:27:7e:
                    a0:94:29:db:02:5a:e4:03:51:16:03:3a:be:57:7d:
                    3b:d1:75:47:84:af:b9:81:43:ab:90:fd:6d:08:d3:
                    e8:5b:80:c5:ca:29:d8:45:58:5f:e4:a3:ed:9f:67:
                    44:0f:1a:41:c9:d7:62:7f:3f
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                EC:F3:09:E8:78:92:D6:41:5F:79:4D:4B:7A:73:AD:FD:8D:12:77:88
            X509v3 Authority Key Identifier:
                keyid:EC:F3:09:E8:78:92:D6:41:5F:79:4D:4B:7A:73:AD:FD:8D:12:77:88
                DirName:/C=CA/ST=Ontario/L=Concord/O=RuggedCom.com/OU=RC/CN=ROS
                serial:CA:01:2D:C0:BF:F9:FD:F2
            X509v3 Basic Constraints:
                CA:TRUE
    Signature Algorithm: sha1WithRSAEncryption
        64:cf:68:6e:9f:19:63:0e:70:49:a6:b2:fd:09:15:6f:96:1d:
        4a:7a:52:c3:46:51:06:83:7f:02:8e:42:b2:dd:21:d2:e9:07:
        5c:c4:4c:ca:c5:a9:10:49:ba:d4:28:fd:fc:9d:a9:0b:3f:a7:
        84:81:37:ca:57:aa:0c:18:3f:c1:b2:45:2a:ed:ad:dd:7f:ad:
        00:04:76:1c:f8:d9:c9:5c:67:9e:dd:0e:4f:e5:e3:21:8b:0b:
        37:39:8b:01:aa:ca:30:0c:f1:1e:55:7c:9c:1b:43:ae:4f:cd:
        e4:69:78:25:5a:a5:f8:98:49:33:39:e3:15:79:44:37:52:da:
        28:dd
```

Section 1.2.2.2
SSH Key Pairs

Controlled versions of ROS support SSH public/private key pairs that conform to the following specifications:

- PEM format
- DSA key pair, 512 to 2048 bits in length

The DSA key pair used in the default key pair and in those generated by ROS uses a public key of 1024 bits in length.

NOTE
DSA keys smaller than 1024 bits in length are not recommended, and support is only included here for compatibility with legacy equipment.

The following (bash) shell script fragment uses the `ssh-keygen` command line utility to generate a 1024 bit DSA key suitable for use in ROS . The resulting `ssh.keys` file, which may then be uploaded to ROS:

```
# DSA key size:
BITS=1024

# Make an SSH key pair:
ssh-keygen -t dsa -b 1024 -N '' -f ssh.keys
```

The following is an example of an SSH key generated by ROS:

```
Private-Key: (1024 bit)
priv:
    00:b2:d3:9d:fa:56:99:a5:7a:ba:1e:91:c5:e1:35:
    77:85:e8:c5:28:36
pub:
    6f:f3:9e:af:e6:d6:fd:51:51:b9:fa:d5:f9:0a:b7:
    ef:fc:d7:7c:14:59:52:48:52:a6:55:65:b7:cb:38:
    2e:84:76:a3:83:62:d0:83:c5:14:b2:6d:7f:cc:f4:
    b0:61:0d:12:6d:0f:5a:38:02:67:a4:b7:36:1d:49:
    0a:d2:58:e2:ff:4a:0a:54:8e:f2:f4:c3:1c:e0:1f:
    9b:1a:ee:16:e0:e9:eb:c8:fe:e8:16:99:e9:61:81:
    ed:e4:f2:58:fb:3b:cb:c3:f5:9a:fa:ed:cd:39:51:
    47:90:5d:6d:1b:27:d5:04:c5:de:57:7e:a7:a3:03:
    e8:fb:0a:d5:32:89:40:12
P:
    00:f4:81:c1:9b:5f:1f:eb:ac:43:2e:db:dd:77:51:
    6e:1c:62:8d:4e:95:c6:e7:b9:4c:fb:39:9c:9d:da:
    60:4b:0f:1f:c6:61:b0:fc:5f:94:e7:45:c3:2b:68:
    9d:11:ba:e1:8a:f9:c8:6a:40:95:b9:93:7c:d0:99:
    96:bf:05:2e:aa:f5:4e:f0:63:02:00:c7:c2:52:c7:
    1a:70:7c:f7:e5:fe:dd:3d:57:02:86:ae:d4:89:20:
    ca:4b:46:80:ea:de:a1:30:11:5c:91:e2:40:d4:a3:
    82:c5:40:3b:25:8e:d8:b2:85:cc:f5:9f:a9:1d:ea:
    0a:ac:77:95:ee:d6:f7:61:e3
Q:
    00:d5:db:48:18:bd:ec:69:99:eb:ff:5f:e1:40:af:
    20:80:6d:5c:b1:23
G:
    01:f9:a1:91:c0:82:12:74:49:8a:d5:13:88:21:3e:
    32:ea:f1:74:55:2b:de:61:6c:fd:dd:f5:e1:c5:03:
    68:b4:ad:40:48:58:62:6c:79:75:b1:5d:42:e6:a9:
    97:86:37:d8:1e:e5:65:09:28:86:2e:6a:d5:3d:62:
    50:06:b8:d3:f9:d4:9c:9c:75:84:5b:db:96:46:13:
    f0:32:f0:c5:cb:83:01:a8:ae:d1:5a:ac:68:fb:49:
    f9:b6:8b:d9:d6:0d:a7:de:ad:16:2b:23:ff:8e:f9:
    3c:41:16:04:66:cf:e8:64:9e:e6:42:9a:d5:97:60:
    c2:e8:9e:f4:bc:8f:6f:e0
```

Section 1.3
Available Services by Port

The following table lists the services available under ROS. This table includes the following information:

- **Services**

The service supported by the device.

- **Port Number**

  The port number associated with the service.

- **Port Open**

  The port state, whether it is always open and cannot be closed, or open only, but can be configured.

  NOTE
  In certain cases, the service might be disabled, but the port can still be open (e.g. TFTP).

- **Port Default**

  The default state of the port (i.e. open or closed).

- **Access Authorized**

  Denotes whether the ports/services are authenticated during access.

Services	Port Number	Port Open	Port Default	Access Authorized	Note
Telnet	TCP/23	Open (configurable)	Closed	Yes	Only available through two management interfaces.
HTTP	TCP/80	Open, redirects to 443	Open	—	
HTTPS	TCP/443	Open	Open	Yes	
RSH	TCP/512	Open (configurable)	Closed	Yes	Only available through two management interfaces.
TFTP	UDP/69	Open (configurable)	Closed	No	Only available through two management interfaces.
SFTP	TCP/22	Open	Open	Yes	Only available through two management interfaces.
SNMP	UDP/161	Open (configurable)	Closed	Yes	Only available through two management interfaces.
SNTP	UDP/123	Open - Always might acts as server	Open	No	Only available through two management interfaces.
SSH	TCP/22	Open	Open	Yes	Only available through two management interfaces.
ICMP	—	Open	Open	No	

Services	Port Number	Port Open	Port Default	Access Authorized	Note
TACACS+	TCP/49 (configurable)	Open (configurable)	Closed	Yes	
RADIUS	UDP/1812 to send (configurable), opens random port to listen to	Open (configurable)	Closed	Yes	Only available through two management interfaces.
Remote Syslog	UDP/514 (configurable)	Open (configurable)	Closed	No	Only available through two management interfaces.
DNP over RawSocket	TCP/21001 to TCP/21016	Open (configurable)	Closed	No	
DNPv3	UDP/20000 TCP/20000	UDP Open; TCP open after configured first time - can not be closed	UDP Open; TCP Closed	No	
RawSocket/Telnet COM	UDP/50001 to UDP/50016 TCP/50001 to TCP/50016	Open (configurable)	Closed	No	
Preemptive RAW Socket	TCP/62001 to TCP/62016	Open (configurable)	Closed	No	
TIN	UDP/51000 TCP/51000	UDP Open; TCP open after configured first time - can not be closed	UDP Open; TCP Closed	No	
WIN	UDP/52000 TCP/52000	UDP Open; TCP open after configured first time - can not be closed	UDP Open; TCP Closed	No	
MICROLOK	UDP/60000	UDP Open; TCP open after configured first time - can not be closed	UDP Open; TCP Closed	No	
MirroredBits	UDP/61001 to UDP/61016	Open (configurable)	Closed	No	
TCP Modbus (Server)	TCP/502	Open	Open	No	Only available through two management interfaces.
TCP Modbus (Switch)	TCP/502	Open (configurable)	Closed	No	
DHCP, DHCP Agent	UDP/67 sending msg if enabled - if received, always come to CPU,	Open	Open	No	

Services	Port Number	Port Open	Port Default	Access Authorized	Note
	dropped if service not configured				
RCDP	—	Open (configurable)	Closed	Yes	

Section 1.4
SNMP Management Interface Base (MIB) Support

ROS supports a variety of standard MIBs, proprietary RUGGEDCOM MIBs and Agent Capabilities MIBs, all for SNMP (Simple Network Management Protocol).

- Section 1.4.1, “Supported Standard MIBs”
- Section 1.4.2, “Supported Proprietary RUGGEDCOM MIBs”
- Section 1.4.3, “Supported Agent Capabilities”

Section 1.4.1
Supported Standard MIBs

ROS supports the following standard MIBs:

Standard	MIB Name	Title
RFC 2578	SNMPv2-SMI	Structure of Management Information Version 2
RFC 2579	SNMPv2-TC	Textual Convention s for SMIv2
RFC 2580	SNMPv2-CONF	Conformance Statements for SMIv2
	IANAifType	Enumerated Values of the ifType Object Defined ifTable defined in IF-MIB
RFC 1907	SNMPv2-MIB	Management Information Base for SNMPv2
RFC 2011	IP-MIB	SNMPv2 Mnagement Information Base for Internet Protocol using SMIv2
RFC 2012	TCP-MIB	SNMPv2 Management Information Base for the Transmission Control Protocol using SMIv2
RFC 2013	UDP-MIB	Management Information Base for the UDP using SMIv2
RFC 1659	RS-232-MIB	Definitions of Managed Objects for RS-232-like Hardware Devices
RFC 2863	IF-MIB	The Interface Group MIB
RFC 2819	RMON-MIB	Remote Network Monitoring (RMON) management Information base
RFC 4188	BRIDGE-MIB	Definitions of Managed Objects for Bridges
RFC 4318	RSTP-MIB	Definitions of Managed Objects for Bridges with Rapid Spanning Tree Protocol
RFC 3411	SNMP-FRAMEWORK-MIB	An Architecture for Describing Simple Network Management Protocol (SNMP) Management Framework

Standard	MIB Name	Title
RFC 3414	SNMP-USER-BASED-SM-MIB	User-based Security Model (USM) for Version 3 of the Simple Network Management Protocol (SNMPv3)
RFC 3415	SNMP-VIEW-BASED-ACM-MIB	View-bsed Access Control Model (VACM) for the Simple Management Protocol (SNMP)
IEEE 802.3ad	IEEE8023-LAG-MIB	Management Information Base Module for Link Aggregation
IEEE 802.1AB-2005	LLDP-MIB	Management Information Base Module for LLDP Configuration, Statistics, Local System Data and Remote Systems Data Components
RFC 4363	Q-BRIDGE-MIB	Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering, and Virtual LAN Extensions

Section 1.4.2
Supported Proprietary RUGGEDCOM MIBs

ROS supports the following proprietary RUGGEDCOM MIBs:

File Name	MIB Name	Description
ruggedcom.mib	RUGGEDCOM-MIB	RUGGEDCOM enterprise SMI
ruggedcomtraps.mib	RUGGEDCOM-TRAPS-MIB	RUGGEDCOM traps definition
rcsysinfo.mib	RUGGEDCOM-SYS-INFO-MIB	General system information about RUGGEDCOM device
rcDot11.mib	RUGGEDCOM-DOT11-MIB	Managemet for wireless interface on RUGGEDCOM device
rcPoe.mib	RUGGEDCOM-POE-MIB	Management for PoE ports on RUGGEDCOM device
rcSerial.mib	RUGGEDCOM-SERIAL-MIB	Managemet for seral ports on RUGGEDCOM device
rcRstp.mib	RUGGEDCOM-STP-MIB	Management for RSTP protocol

Section 1.4.3
Supported Agent Capabilities

ROS supports the following agent capabilities for the SNMP agent:

NOTE
For information about agent capabilities for SNMPv2, refer to RFC 2580 [http://tools.ietf.org/html/rfc2580].

File Name	MIB Name	Supported MIB
rcsnmpv2AC.mib	RC-SNMPv2-MIB-AC	SNMPv2-MIB
rcudpmibAC.mib	RC-UDP-MIB-AC	UDP-MIB
rctcpmibAC.mib	RC-TCP-MIB-AC	TCP-MIB

File Name	MIB Name	Supported MIB
rcSnmpUserBasedSmMibAC.mib	RC-SNMP-USER-BASED-SM-MIB-AC	SNMP-USER-BASED-SM-MIB-AC
rcSnmpViewBasedAcmMibAC.mib	RC-SNMP-VIEW-BASED-ACM-MIB-AC	SNMP-VIEW-BASED-ACM-MIB-AC
rcifmibAC.mib	RC-IF-MIB-AC	IF-MIB
rcbridgemibAC.mib	RC-BRIDGE-MIB-AC	BRIDGE-MIB
rcrmonmibAC.mib	RC-RMON-MIB-AC	RMON-MIB
rcqbridgemibAC.mib	RC-Q-BRIDGE-MIB-AC	Q-BRIDGE-MIB
rcipmibAC.mib	RC-IP-MIB-AC	IP-MIB
rclldpmibAC.mib	RC-LLDP-MIB-AC	LLDP-MIB
rclagmibAC.mib	RC-LAG-MIB-AC	IEEE8023-LAG-MIB
rcrstpmibAC.mib	RC_RSTP-MIB-AC	RSTP-MIB
rcrcdot11AC.mib	RC-RUGGEDCOM-DOT11-MIB-AC	RUGGEDCOM-DOT11- MIB
rcrcpoeAC.mib	RC-RUGGEDCOM-POE-MIB-AC	RUGGEDCOM-POE-MIB
rcrcrstpmibAC.mib	RC-RUGGEDCOM-STP-AC-MIB	RUGGEDCOM-STP-MIB
rcrcsysinfomibAC.mib	RC-RUGGEDCOM-SYS-INFO-MIB-AC	RUGGEDCOM-SYS-INFO-MIB
rcrctrapsmibAC.mib	RC-RUGGEDCOM-TRAPS-MIB-AC	RUGGEDCOM-TRAPS-MIB
rcrs232mibAC.mib	RUGGEDCOM_RS-232-MIB-AC	RS-232-MIB
rcserialmibAC.mib	RC-RUGGEDCOM-SERIAL-MIB-AC	RUGGEDCOM-SERIAL-MIB

Section 1.5
SNMP Traps

The device generates the following standard traps:

Table: Standard Traps

Trap	MIB
linkDown	IF-MIB
linkUp	
authenticationFailure	SNMPv2-MIB
coldStart	
newRoot	BRIDGE-MIB
topologyChage	
risingAlarm	RMON-MIB
fallingAlarm	
lldpRemoteTablesChange	LLDP-MIB

The device also generates the following proprietary traps:

Table: Proprietary Traps

Trap	MIB
genericTrap	RUGGEDCOM-TRAPS-MIB
powerSupplyTrap	
swUpgradeTrap	
cfgChangeTrap	
weakPasswordTrap	
defaultKeysTrap	

Generic traps carry information about events in their severity and description objects. They are sent at the same time an alarm is generated for the device. The following are examples of RUGGEDCOM generic traps:

NOTE
Information about generic traps can be retrieved using the CLI command **`alarms`**. *For more information about the* **`alarms`** *command, refer to* *Section 2.6.1, "Available CLI Commands"*.

Table: Generic Traps

Trap	Severity
heap error	Alert
NTP server failure	notification
real time clock failure	Error
failed password	Warning
MAC address not learned by switch fabric	Warning
BootP client: TFTP transfer failure	Error
received looped back BPDU	Error
received two consecutive confusing BPDUs on port, forcing down	Error

The device generates the following traps when specific events occur:

Table: Event-Based Traps

Trap	MIB	Event
rcRstpNewTopology	RUGGEDCOM-STP-MIB	This trap is generated when the device topology becomes stable after a topology change occurs on a switch port.

Section 1.6

ModBus Management Support

Modbus management support in RUGGEDCOM devices provides a simple interface for retrieving basic status information. ModBus support simplifies the job of SCADA (Supervisory Control and Data Acquisition) system integrators by providing familiar protocols for retrieving RUGGEDCOM device information. ModBus provides mostly read-only status information, but there are some writable registers for operator commands.

The ModBus protocol PDU (Protocol Data Unit) format is as follows:

Function Code	Data

The following sections describe the support for ModBus management:

- Section 1.6.1, “ModBus Function Codes”
- Section 1.6.2, “ModBus Memory Map”
- Section 1.6.3, “ModBus Memory Formats”

Section 1.6.1

ModBus Function Codes

RUGGEDCOM devices support the following ModBus function codes for device management through ModBus:

NOTE
While RUGGEDCOM devices have a variable number of ports, not all registers and bits apply to all products.

Registers that are not applicable to a particular device return a zero (0) value. For example, registers referring to serial ports are not applicable to RUGGEDCOM switch devices.

Read Input Registers or Read Holding Registers — 0x04 or 0x03

Example PDU Request

Function Code	1 Byte	0x04(0x03)
Starting Address	2 Bytes	0x0000 to 0xFFFF (Hexadecimal) 128 to 65535 (Decimal)
Number of Input Registers	2 Bytes	Bytes 0x0001 to 0x007D

Example PDU Response

Function Code	1 Byte	0x04(0x03)
Byte Count	1 Byte	2 x N^a
Number of Input Registers	N^a x 2 Bytes	

[a] *The number of input registers*

Write Multiple Registers — 0x10

Example PDU Request

Function Code	1 Byte	0x10
Starting Address	2 Bytes	0x0000 to 0xFFFF
Number of Input Registers	2 Bytes	Bytes 0x0001 to 0x0079
Byte Count	1 Byte	2 x N^b
Registers Value	N^b x 2 Bytes	Value of the register

[b] *The number of input registers*

Example PDU Response

Function Code	1 Byte	0x10

Starting Address	2 Bytes	0x0000 to 0xFFFF
Number of Registers	2 Bytes	1 to 121 (0x79)

Section 1.6.2
ModBus Memory Map

The following details how ModBus process variable data is mapped.

Product Info

The following data is mapped to the *Productinfo* table:

Address	#Registers	Description (Reference Table in UI)	R/W	Format
0000	16	Product Identification	R	Text
0010	32	Firmware Identification	R	Text
0040	1	Number of Ethernet Ports	R	Uint16
0041	1	Number of Serial Ports	R	Uint16
0042	1	Number of Alarms	R	Uint16
0043	1	Power Supply Status	R	PSStatusCmd
0044	1	FailSafe Relay Status	R	TruthValue
0045	1	ErrorAlarm Status	R	TruthValue

Product Write Register

The following data is mapped to various tables:

Address	#Registers	Description (Reference Table in UI)	R/W	Format
0080	1	Clear Alarms	W	Cmd
0081	2	Reset Ethernet Ports	W	PortCmd
0083	2	Clear Ethernet Statistics	W	PortCmd
0085	2	Reset Serial Ports	W	PortCmd
0087	2	Clear Serial Port Statistics	W	PortCmd

Alarms

The following data is mapped to the *alarms* table:

Address	#Registers	Description (Reference Table in UI)	R/W	Format
0100	64	Alarm 1	R	Alarm
0140	64	Alarm 2	R	Alarm
0180	64	Alarm 3	R	Alarm
01C0	64	Alarm 4	R	Alarm
0200	64	Alarm 5	R	Alarm

Address	#Registers	Description (Reference Table in UI)	R/W	Format
0240	64	Alarm 6	R	Alarm
0280	64	Alarm 7	R	Alarm
02C0	64	Alarm 8	R	Alarm

Ethernet Port Status

The following data is mapped to the *ethPortStats* table:

Address	#Registers	Description (Reference Table in UI)	R/W	Format
03FE	2	Port Link Status	R	PortCmd

Ethernet Statistics

The following data is mapped to the *rmonStats* table:

Address	#Registers	Description (Reference Table in UI)	R/W	Format
0400	2	Port s1/p1 Statistics - Ethernet In Packets	R	Uinst32
0402	2	Port s1/p2 Statistics - Ethernet In Packets	R	Uinst32
0404	2	Port s1/p3 Statistics - Ethernet In Packets	R	Uinst32
0406	2	Port s1/p4 Statistics - Ethernet In Packets	R	Uinst32
0408	2	Port s2/p1 Statistics - Ethernet In Packets	R	Uinst32
040A	2	Port s2/p2 Statistics - Ethernet In Packets	R	Uinst32
040C	2	Port s2/p3 Statistics - Ethernet In Packets	R	Uinst32
040E	2	Port s2/p4 Statistics - Ethernet In Packets	R	Uinst32
0410	2	Port s3/p1 Statistics - Ethernet In Packets	R	Uinst32
0412	2	Port s3/p2 Statistics - Ethernet In Packets	R	Uinst32
0414	2	Port s3/p3 Statistics - Ethernet In Packets	R	Uinst32
0416	2	Port s3/p4 Statistics - Ethernet In Packets	R	Uinst32
0418	2	Port s4/p1 Statistics - Ethernet In Packets	R	Uinst32
041A	2	Port s4/p2 Statistics - Ethernet In Packets	R	Uinst32
041C	2	Port s4/p3 Statistics - Ethernet In Packets	R	Uinst32
041E	2	Port s4/p4 Statistics - Ethernet In Packets	R	Uinst32
0420	2	Port s5/p1 Statistics - Ethernet In Packets	R	Uinst32
0422	2	Port s5/p2 Statistics - Ethernet In Packets	R	Uinst32
0424	2	Port s5/p3 Statistics - Ethernet In Packets	R	Uinst32
0426	2	Port s5/p4 Statistics - Ethernet In Packets	R	Uinst32
0428	2	Port s6/p1 Statistics - Ethernet In Packets	R	Uinst32
042A	2	Port s6/p2 Statistics - Ethernet In Packets	R	Uinst32
042C	2	Port s6/p3 Statistics - Ethernet In Packets	R	Uinst32
042E	2	Port s6/p4 Statistics - Ethernet In Packets	R	Uinst32

Address	#Registers	Description (Reference Table in UI)	R/W	Format
0430	2	Port s7/p1 Statistics - Ethernet In Packets	R	Uinst32
0432	2	Port s7/p2 Statistics - Ethernet In Packets	R	Uinst32
0434	2	Port s8/p1 Statistics - Ethernet In Packets	R	Uinst32
0436	2	Port s8/p2 Statistics - Ethernet In Packets	R	Uinst32
0440	2	Port s1/p1 Statistics - Ethernet Out Packets	R	Uinst32
0442	2	Port s1/p2 Statistics - Ethernet Out Packets	R	Uinst32
0444	2	Port s1/p3 Statistics - Ethernet Out Packets	R	Uinst32
0446	2	Port s1/p4 Statistics - Ethernet Out Packets	R	Uinst32
0448	2	Port s2/p1 Statistics - Ethernet Out Packets	R	Uinst32
044A	2	Port s2/p2 Statistics - Ethernet Out Packets	R	Uinst32
044C	2	Port s2/p3 Statistics - Ethernet Out Packets	R	Uinst32
044E	2	Port s2/p4 Statistics - Ethernet Out Packets	R	Uinst32
0450	2	Port s3/p1 Statistics - Ethernet Out Packets	R	Uinst32
0452	2	Port s3/p2 Statistics - Ethernet Out Packets	R	Uinst32
0454	2	Port s3/p3 Statistics - Ethernet Out Packets	R	Uinst32
0456	2	Port s3/p4 Statistics - Ethernet Out Packets	R	Uinst32
0458	2	Port s4/p1 Statistics - Ethernet Out Packets	R	Uinst32
045A	2	Port s4/p2 Statistics - Ethernet Out Packets	R	Uinst32
045C	2	Port s4/p3 Statistics - Ethernet Out Packets	R	Uinst32
045E	2	Port s4/p4 Statistics - Ethernet Out Packets	R	Uinst32
0460	2	Port s5/p1 Statistics - Ethernet Out Packets	R	Uinst32
0462	2	Port s5/p2 Statistics - Ethernet Out Packets	R	Uinst32
0464	2	Port s5/p3 Statistics - Ethernet Out Packets	R	Uinst32
0466	2	Port s5/p4 Statistics - Ethernet Out Packets	R	Uinst32
0468	2	Port s6/p1 Statistics - Ethernet Out Packets	R	Uinst32
046A	2	Port s6/p2 Statistics - Ethernet Out Packets	R	Uinst32
046C	2	Port s6/p3 Statistics - Ethernet Out Packets	R	Uinst32
046E	2	Port s6/p4 Statistics - Ethernet Out Packets	R	Uinst32
0470	2	Port s7/p1 Statistics - Ethernet Out Packets	R	Uinst32
0472	2	Port s7/p2 Statistics - Ethernet Out Packets	R	Uinst32
0474	2	Port s8/p1 Statistics - Ethernet Out Packets	R	Uinst32
0476	2	Port s8/p2 Statistics - Ethernet Out Packets	R	Uinst32
0480	2	Port s1/p1 Statistics - Ethernet In Packets	R	Uinst32
0482	2	Port s1/p2 Statistics - Ethernet In Packets	R	Uinst32

Address	#Registers	Description (Reference Table in UI)	R/W	Format
0484	2	Port s1/p3 Statistics - Ethernet In Packets	R	Uinst32
0486	2	Port s1/p4 Statistics - Ethernet In Packets	R	Uinst32
0488	2	Port s2/p1 Statistics - Ethernet In Packets	R	Uinst32
048A	2	Port s2/p2 Statistics - Ethernet In Packets	R	Uinst32
048C	2	Port s2/p3 Statistics - Ethernet In Packets	R	Uinst32
048E	2	Port s2/p4 Statistics - Ethernet In Packets	R	Uinst32
0490	2	Port s3/p1 Statistics - Ethernet In Packets	R	Uinst32
0492	2	Port s3/p2 Statistics - Ethernet In Packets	R	Uinst32
0494	2	Port s3/p3 Statistics - Ethernet In Packets	R	Uinst32
0496	2	Port s3/p4 Statistics - Ethernet In Packets	R	Uinst32
0498	2	Port s4/p1 Statistics - Ethernet In Packets	R	Uinst32
049A	2	Port s4/p2 Statistics - Ethernet In Packets	R	Uinst32
049C	2	Port s4/p3 Statistics - Ethernet In Packets	R	Uinst32
049E	2	Port s4/p4 Statistics - Ethernet In Packets	R	Uinst32
04A0	2	Port s5/p1 Statistics - Ethernet In Packets	R	Uinst32
04A2	2	Port s5/p2 Statistics - Ethernet In Packets	R	Uinst32
04A4	2	Port s5/p3 Statistics - Ethernet In Packets	R	Uinst32
04A6	2	Port s5/p4 Statistics - Ethernet In Packets	R	Uinst32
04A8	2	Port s6/p1 Statistics - Ethernet In Packets	R	Uinst32
04AA	2	Port s6/p2 Statistics - Ethernet In Packets	R	Uinst32
04AC	2	Port s6/p3 Statistics - Ethernet In Packets	R	Uinst32
04AE	2	Port s6/p4 Statistics - Ethernet In Packets	R	Uinst32
04B0	2	Port s7/p1 Statistics - Ethernet In Packets	R	Uinst32
04B2	2	Port s7/p2 Statistics - Ethernet In Packets	R	Uinst32
04B4	2	Port s8/p1 Statistics - Ethernet In Packets	R	Uinst32
04B6	2	Port s8/p2 Statistics - Ethernet In Packets	R	Uinst32
04C0	2	Port s1/p1 Statistics - Ethernet Out Packets	R	Uinst32
04C2	2	Port s1/p2 Statistics - Ethernet Out Packets	R	Uinst32
04C4	2	Port s1/p3 Statistics - Ethernet Out Packets	R	Uinst32
04C6	2	Port s1/p4 Statistics - Ethernet Out Packets	R	Uinst32
04C8	2	Port s2/p1 Statistics - Ethernet Out Packets	R	Uinst32
04CA	2	Port s2/p2 Statistics - Ethernet Out Packets	R	Uinst32
04CC	2	Port s2/p3 Statistics - Ethernet Out Packets	R	Uinst32
04CE	2	Port s2/p4 Statistics - Ethernet Out Packets	R	Uinst32

Address	#Registers	Description (Reference Table in UI)	R/W	Format
04D0	2	Port s3/p1 Statistics - Ethernet Out Packets	R	Uinst32
04D2	2	Port s3/p2 Statistics - Ethernet Out Packets	R	Uinst32
04D4	2	Port s3/p3 Statistics - Ethernet Out Packets	R	Uinst32
04D6	2	Port s3/p4 Statistics - Ethernet Out Packets	R	Uinst32
04D8	2	Port s4/p1 Statistics - Ethernet Out Packets	R	Uinst32
04DA	2	Port s4/p2 Statistics - Ethernet Out Packets	R	Uinst32
04DC	2	Port s4/p3 Statistics - Ethernet Out Packets	R	Uinst32
04DE	2	Port s4/p4 Statistics - Ethernet Out Packets	R	Uinst32
04E0	2	Port s5/p1 Statistics - Ethernet Out Packets	R	Uinst32
04E2	2	Port s5/p2 Statistics - Ethernet Out Packets	R	Uinst32
04E4	2	Port s5/p3 Statistics - Ethernet Out Packets	R	Uinst32
04E6	2	Port s5/p4 Statistics - Ethernet Out Packets	R	Uinst32
04E8	2	Port s6/p1 Statistics - Ethernet Out Packets	R	Uinst32
04EA	2	Port s6/p2 Statistics - Ethernet Out Packets	R	Uinst32
04EC	2	Port s6/p3 Statistics - Ethernet Out Packets	R	Uinst32
04EE	2	Port s6/p4 Statistics - Ethernet Out Packets	R	Uinst32
04F0	2	Port s7/p1 Statistics - Ethernet Out Packets	R	Uinst32
04F2	2	Port s7/p2 Statistics - Ethernet Out Packets	R	Uinst32
04F4	2	Port s8/p1 Statistics - Ethernet Out Packets	R	Uinst32
04F6	2	Port s8/p2 Statistics - Ethernet Out Packets	R	Uinst32

Serial Statistics

The following data is mapped to the *uartPortStatus* table:

Address	#Registers	Description (Reference Table in UI)	R/W	Format
0600	2	Port 1 Statistics – Serial In characters	R	Uint32
0602	2	Port 2 Statistics – Serial In characters	R	Uint32
0604	2	Port 3 Statistics – Serial In characters	R	Uint32
0606	2	Port 4 Statistics – Serial In characters	R	Uint32
0640	2	Port 1 Statistics – Serial Out characters	R	Uint32
0642	2	Port 2 Statistics – Serial Out characters	R	Uint32
0644	2	Port 3 Statistics – Serial Out characters	R	Uint32
0646	2	Port 4 Statistics – Serial Out characters	R	Uint32
0680	2	Port 1 Statistics – Serial In Packets	R	Uint32
0682	2	Port 2 Statistics – Serial In Packets	R	Uint32
0684	2	Port 3 Statistics – Serial In Packets	R	Uint32

Address	#Registers	Description (Reference Table in UI)	R/W	Format
0686	2	Port 4 Statistics – Serial In Packets	R	Uint32
06C0	2	Port 1 Statistics – Serial Out Packets	R	Uint32
06C2	2	Port 2 Statistics – Serial Out Packets	R	Uint32
06C4	2	Port 3 Statistics – Serial Out Packets	R	Uint32
06C6	2	Port 4 Statistics – Serial Out Packets	R	Uint32

Section 1.6.3
ModBus Memory Formats

The following ModBus memory formats are supported by Siemens:

- Section 1.6.3.1, “Text”
- Section 1.6.3.2, “Cmd”
- Section 1.6.3.3, “Uint16”
- Section 1.6.3.4, “Uint32”
- Section 1.6.3.5, “PortCmd”
- Section 1.6.3.6, “Alarm”
- Section 1.6.3.7, “PSStatusCmd”
- Section 1.6.3.8, “TruthValues”

Section 1.6.3.1
Text

The Text format provides a simple ASCII representation of the information related to the product. The most significant register byte of an ASCII characters comes first.

For example, consider a *Read Multiple Registers* request to read Product Identification from location 0x0000.

0x04	0x00	0x00	0x00	0x08

The response may look like:

0x04	0x10	0x53	0x59	0x53	0x54	0x45	0x4D	0x20	0x4E	0x41	0x4D	0x45
0x00	0x00	0x00	0x00	0x00								

In this example, starting from byte 3 until the end, the response presents an ASCII representation of the characters for the product identification, which reads as *SYSTEM NAME*. Since the length of this field is smaller than eight registers, the rest of the field is filled with zeros (0).

Section 1.6.3.2
Cmd

The Cmd format instructs the device to set the output to either *true* or *false*. The most significant byte comes first.

- FF 00 hex requests output to be True
- 00 00 hex requests output to be False
- Any value other than the suggested values does not affect the requested operation

For example, consider a *Write Multiple Registers* request to clear alarms in the device.

0x10	0x00	0x80	0x00	0x01	2	0xFF	0x00

- FF 00 for register 00 80 clears the system alarms
- 00 00 does not clear any alarms

The response may look like:

0x10	0x00	0x80	0x00	0x01

Section 1.6.3.3
Uint16

The Uint16 format describes a Standard ModBus 16 bit register.

Section 1.6.3.4
Uint32

The Uint32 format describes Standard 2 ModBus 16 bit registers. The first register holds the most significant 16 bits of a 32 bit value. The second register holds the least significant 16 bits of a 32 bit value.

Section 1.6.3.5
PortCmd

The PortCmd format describes a bit layout per port, where 1 indicates the requested action is true, and 0 indicates the requested action is false.

PortCmd provides a bit layout of a maximum of 32 ports. Therefore, it uses two ModBus regsiters:

- The first ModBus register corresponds to ports 1 – 16
- The second ModBus register corresponds to ports 17 – 32 for a particular action

Bits that do not apply to a particular product are always set to zero (0).

A bit value of 1 indicates that the requested action is true. For example, the port is *up*.

A bit value of 0 indicates that the requested action is false. For example, the port is *down*.

Reading Data Using PortCmd

To understand how to read data using PortCmd, consider a ModBus Request to read multiple registers from locatoin 0x03FE.

0x04	0x03	0xFE	0x00	0x02

The response depends on how many parts are available on the device. For example, if the maximum number of ports on a connected RUGGEDCOM device is 20, the response would be similar to the following:

0x04	0x04	0xF2	0x76	0x00	0x05

In this example, bytes 3 and 4 refer to register 1 at location 0x03FE, and represent the status of ports 1 – 16. Bytes 5 and 6 refer to register 2 at location 0x03FF, and represent the status of ports 17 – 32. The device only has 20 ports, so byte 6 contains the status for ports 17 – 20 starting from right to left. The rest of the bites in register 2 corresponding to the non-existing ports 21 – 31 are zero (0).

Performing Write Actions Using PortCmd

To understand how data is written using PortCmd, consider a Write Multiple Register request to clear Ethernet port statistics:

0x10	0x00	0x83	0x00	0x01	2	0x55	0x76	0x00	0x50

A bit value of 1 clears Ethernet statistics on the corresponding port. A bit value of 0 does not clear the Ethernet statistics.

0x10	0x00	0x81	0x00	0x02

Section 1.6.3.6

Alarm

The Alarm format is another form of text description. Alarm text corresponds to the alarm description from the table holding all of the alarms. Similar to the Text format, this format returns an ASCII representation of alarms.

NOTE
Alarms are stacked in the device in the sequence of their occurence (i.e. Alarm 1, Alarm 2, Alarm 3, etc.).

The first eight alarms from the stack can be returned, if they exist. A zero (0) value is returned if an alarm does not exist.

Section 1.6.3.7

PSStatusCmd

The PSStatusCmd format describes a bit layout for providing the status of available power supplies. Bits 0-4 of the lower byte of the register are used for this purpose.

- Bits 0-1: Power Supply 1 Status
- Bits 2-3: Power Supply 2 Status

Other bits in the register do not provide any system status information.

Bit Value	Description
01	Power Supply not present (01 = 1)
10	Power Supply is functional (10 = 2)
11	Power Supply is not functional (11 = 3)

The values used for power supply status are derived from the RUGGEDCOM-specific SNMP MIB.

Reading the Power Supply Status from a Device Using PSStatusCmd

To understand how to read the power supply status from a device using PSStatusCmd, consider a ModBus Request to read multiple registers from location 0x0043.

0x04	0x00	0x43	0x00	0x01

The response may look like:

0x04	0x02	0x00	0x0A

The lower byte of the register displays the power supply's status. In this example, both power supplies in the unit are functional.

Section 1.6.3.8
TruthValues

The Truthvalues format represents a true or false status in the device:

- 1 indicates the corresponding status for the device to be true
- 2 indicates the corresponding status for the device to be false

Reading the FailSafe Relay Status From a Device Using TruthValue

To understand how to use the TruthValue format to read the FailSafe Relay status from a device, consider a ModBus request to read multiple registers from location 0x0044.

0x04	0x00	0x44	0x00	0x01

The response may look like:

0x04	0x02	0x00	0x01

The register's lower byte shows the FailSafe Relay status. In this example, the FailSafe Relay is energized.

Reading the ErrorAlarm Status From a Device Using TruthValue

To understand how to use the TruthValue format to read the ErrorAlarm status from a device, conside a ModBus request to read mulitple registers from location 0x0045.

0x04	0x00	0x45	0x00	0x01

The response may look like:

0x04	0x02	0x00	0x01

The register's lower byte shows the ErrorAlarm status. In this example, there is no active ERROR, ALERT or CRITICAL alarm in the device.

Section 1.7
Certificate and Key Requirements

Users are able to load custom and unique SSL certificates and SSL/SSH keys in ROS or use the certificates and keys provided by ROS.

There are three types of certificates and keys:

NOTE
Default and auto-generated SSH keys are not available for Non-Controlled (NC) versions of ROS.

- **Default**

Each ROS device is shipped with an SSL certificate and RSA key pair, and a DSA key pair for SSH that are unique to software version. If a valid SSL certificate or SSL/SSH keys are not available on the device, the default certificate and keys are used immediately so that SSH and SSL (https) sessions can be served.

- **Auto-Generated**

  If a default SSL certificate and SSL/SSH keys are in use, ROS immediately begins to generate a unique certificate and SSL/SSH keys for the device in the background. This process takes approximately 5 minutes to complete (depending on how busy the device is at the time) following the startup of the device. If a custom certificate and keys are loaded while auto-generated certificates and keys are being generated, the generator will abort and the custom certificate and keys and will be used.

- **User-Generated (Recommended)**

  Custom certificates and keys are the most secure option. They give the user complete control over certificate and key management, allow for certificates signed by a public or local certificate authority, controlled distribution of public SSH keys to network hosts that need them, and more.

NOTE
The RSA key pair must be added to the `ssl.crt` *file after the SSL certificate.*

For SSL, ROS requires an X.509 certificate in standard PEM format and an RSA key pair. The certificate may be self-signed or signed by a separate authoriy. The RSA key must be between 512 and 2048 bits in length. The certificate and keys must be combined in a single `ssl.crt` file and uploaded to the device.

The following is an example of a combined SSL certificate and key:

```
-----BEGIN CERTIFICATE-----
MIIC9jCCAl+gAwIBAgIJAJh6rrehMt3iMA0GCSqGSIb3DQEBBQUAMIGuMQswCQYD
VQQGEwJDQTEQMA4GA1UECBMHT250YXJpbzEQMA4GA1UEBxMHQ29uY29yZDESMBAG
A1UEChMJUnVnZ2VkY29tMRkwFwYDVQQLExBDdXN0b211ciBTdXBwb3J0MSYwJAYD
VQQDEx1XUy1NSUxBTkdPVkFOLlJVR0dFRENPTS5MT0NBTDEkMCIGCSqGSIb3DQEJ
ARYVc3VwcG9ydEBydWdnZWRjb20uY29tMB4XDTEyMTAyMzIxMTA1M1oXDTE3MTAy
MjIxMTA1M1owgZwxCzAJBgNVBAYTAlVTMRAwDgYDVQQIEwdPbnRhcmlvMRAwDgYD
VQQHEwdDb25jb3JkMRIwEAYDVQQKEwlSdWdnZWRDb20xGTAXBgNVBAsTEEN1c3Rv
bWVyIFN1cHBvcnQxFDASBgNVBAMTCzE5Mi4xNjguMS4yMSQwIgYJKoZIhvcNAQkB
FhVTdXBwb3J0QHJ1Z2dlZGNvbS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
AoGBALfE4eh2aY+CE3W5a4Wz1Z1RGRP02COHt153wFFrU8/fFQXNhKlQirlAHbNT
RSwcTR8ZFapivwYDivn0ogOGFXknYP90gv2oIaSVY08FqZkJW77g3kzkv/8Zrw3m
W/cBsZJ8SyKLIDfy401HkHpDOle5NsQFSrziGUPjAOIvvx4rAgMBAAGjLDAqMAkG
A1UdEwQCMAAwHQYDVR0OBBYEFER0utgQOifnrflnDtsqNcnvRB0XMA0GCSqGSIb3
DQEBBQUAA4GBAHtBsNZuh8tB3kdqR7Pn+XidCsD70YnI7w0tiy9yiRRhARmVXH8h
5Q1rOeHceri3JFFIOxIxQt4KgCUYJLu+c9Esk/nXQQar3zR7IQCt0qOABPkviiY8
c3ibVbhJjLpR2vNW4xRAJ+HkNNtBOg1xUlp4vOmJ2syYZR+7XAy/OP/S
-----END CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY-----
MIICXAIBAAKBgQC3xOHodmmPghN1uWuFs9WdURkT9Ngjh7ded8BRa1PP3xUFzYSp
UIq5QB2zU0UsHE0fGRWqYr8GA4r59KIDhhV5J2D/dIL9qCGklWNPBamZCVu+4N5M
5L//Ga8N5lv3AbGSfEsiiyA38uNNR5B6QzpXuTbEBUq84hlD4wDiL78eKwIDAQAB
AoGBAI2CXHuHg23wuk9zAusoOhw0MN1/M1jYz0k9aajIvvdZT3Tyd29yCADy8GwA
eUmoWXLS/C4CcBqPa9til8ei3rDn/w8dveVHsi9FXjtVSYqN+ilKw+moMAjZy4kN
/kpdpHMohwv/909VWR1AZbr+YTxaG/++tKl5bqXnZl4wHF8xAkEA5vwut8USRg2/
TndOt1e8ILEQNHvHQdQr2et/xNH4ZEo7mqot6skkCD1xmxA6XG64hR3BfxFSZcew
Wr4SOFGCtQJBAMurr5FYPJRFGzPM3HwcpAaaMIUtPwNyTtTjywlYcUI7iZVVfbdx
4B7qOadPybTg7wqUrGVkPSzzQelz9YCSSV8CQFqpIsEYhbqfTLZEl83YjsuaE801
xBivaWLIT0b2TvM2O7zSDOG5fv4I990v+mgrQRtmeXshVmEChtKnBcm7HH0CQE6B
2WUfLArDMJ8hAoRczeU1nipXrIh5kWWCgQsTKmUrafdEQvdpT8ja5GpX2Rp98eaU
NHfI0cP36JpCdome2eUCQDZN9OrTgPfeDIXzyOiUUwFlzS1idkUGL9nH86iuPnd7
WVF3rV9Dse30sVEk63Yky8uKUy7yPUNWldG4U5vRKmY=
-----END RSA PRIVATE KEY-----
```

For SSH, ROS requires a DSA key pair in PEM format. The DSA key must be between 512 and 2048 bits in length for Controlled versions. The key file is uploaded to the `ssh.keys` flash file on the device.

The following is an example of a PEM formatted SSH key:

```
-----BEGIN DSA PRIVATE KEY-----
MIIBuwIBAAKBgQD0gcGbXx/rrEMu2913UW4cYo1OlcbnuUz7OZyd2mBLDx/GYbD8
X5TnRcMraJ0RuuGK+chqQJW5k3zQmZa/BS6q9U7wYwIAx8JSxxpwfPfl/t09VwKG
rtSJIMpLRoDq3qEwEVyR4kDUo4LFQDsljtiyhcz1n6kd6gqsd5Xu1vdh4wIVANXb
SBi97GmZ6/9f4UCvIIBtXLEjAoGAAfmhkcCCEnRJitUTiCE+MurxdFUr3mFs/d31
4cUDaLStQEhYYmx5dbFdQuap14Y32B7lZQkohi5q1T1iUAa40/nUnJx1hFvblkYT
8DLwxcuDAaiu0VqsaPtJ+baL2dYNp96tFisj/475PEEWBGbP6GSe5kKa1Zdgwuie
9LyPb+ACgYBv856v5tb9UVG5+tX5Crfv/Nd8FFlSSFKmVWW3yzguhHajg2LQg8UU
sm1/zPSwYQ0SbQ9aOAJnpLc2HUkK0lji/0oKVI7y9MMc4B+bGu4W4OnryP7oFpnp
YYHt5PJY+zvLw/Wa+u3NOVFHkF1tGyfVBMXeV36nowPo+wrVMolAEgIVALLTnfpW
maV6uh6RxeE1d4XoxSg2
-----END DSA PRIVATE KEY-----
```

For more information about encryption key management, refer to Section 1.2, “Security Recommendations and Considerations”.

2 Using ROS

This chapter describes how to use the ROS interface. It describes the following tasks:

- Section 2.1, “Connecting to ROS”
- Section 2.2, “Logging In”
- Section 2.3, “Logging Out”
- Section 2.4, “Using the Web Interface”
- Section 2.5, “Using the Console Interface”
- Section 2.6, “Using the Command Line Interface”
- Section 2.7, “Selecting Ports in ROS”
- Section 2.8, “Managing the Flash File System”
- Section 2.9, “Accessing BIST Mode”

Section 2.1

Connecting to ROS

The following describes the various methods for connecting the device:

- Section 2.1.1, “Connecting Directly”
- Section 2.1.2, “Connecting via the Network”

Section 2.1.1

Connecting Directly

ROS can be accessed through a direct serial console or Ethernet connection for management and troubleshooting purposes. A console connection provides access to the console interface and CLI.

To establish a serial connection to the device, do the following:

1. Connect a workstation (either a terminal or computer running terminal emulation software) to the RS232 serial console port on the device. For more information about the RS232 serial console port, refer to the *RMC30 Installation Guide*.

   NOTE
   The baud rate for the device is printed on the chassis exterior near the RS232 serial console port.

2. Configure the workstation as follows:
   - Speed (baud): 57600
   - Data Bits: 8
   - Parity: None

- Flow Control: Off
- Terminal ID: VT100
- Stop Bit: 1

3. Connect to the device. Once the connection is established, the login form appears. For more information about logging in to the device, refer to Section 2.2, “Logging In”.

Section 2.1.2
Connecting via the Network

ROS can be accessed over the network either through a Web browser, terminal or a workstation running terminal emulation software.

Using a Web Browser

Web browsers provide a secure connection to the Web interface for ROS using the SSL (Secure Socket Layer) communication method. SSL encrypts traffic exchanged with its clients.

The ROS Web server guarantees that all communications with the client are private. If a client requests access through an insecure HTTP port, the client is automatically rerouted to the secure port. Access to the Web server through SSL will only be granted to clients that provide a valid user name and password.

To establish a connection through a Web browser, do the following:

1. On the workstation being used to access the device, configure an Ethernet port to use an IP address falling within the subnet of the device. The default IP address is 192.168.0.1/24.

   For example, to configure the device to connect to one of the available Ethernet ports, assign an IP address to the Ethernet port on the workstation in the range of 192.168.0.3 to 192.168.0.254.

2. Open a Web browser. For a list of recommended Web browsers, refer to the section called “System Requirements”.

   IMPORTANT!
   Upon connecting to the device, some Web browsers may report the Web server's certificate cannot be verified against any known certificates. This is expected behavior, and it is safe to instruct the browser to accept the certificate. Once the certificate is accepted, all communications with the Web server through that browser will be secure.

3. In the address bar, type the IP address for the port that is connected to the network. For example, to access the device using its factory default IP address, type **`https://192.168.0.1`** and press **Enter**. Once the connection is established, the login screen for the Web interface appears.

   For more information about logging in to the device, refer to Section 2.2, “Logging In”. For more information about the Web interface, refer to Section 2.4, “Using the Web Interface”.

Using a Terminal or Terminal Emulation Software

A terminal or computer running terminal emulation software provides secure access to the console interface for ROS through a Telnet, RSH (Remote Shell) or SSH (Secure Shell) service.

NOTE
IP services can be restricted to control access to the device. For more information, refer to Section 3.8, “Configuring IP Services”.

To establish a connection through a terminal or terminal emulation software, do the following:

1. Select the service (i.e. Telnet, RSH or SSH).
2. Enter the IP address for the port that is connected to the network.
3. Connect to the device. Once the connection is established, the login form appears. For more information about logging in to the device, refer to Section 2.2, “Logging In”.

Section 2.2
Logging In

To log in to the device, do the following:

1. Connect to the device either directly or through a Web browser. For more information about how to connect to the device, refer to Section 2.1, “Connecting to ROS”.

   Once the connection is established, the login form appears.

Figure 1: SSH Login Screen (Console Interface)

1. User Name Box **2.** Password Box

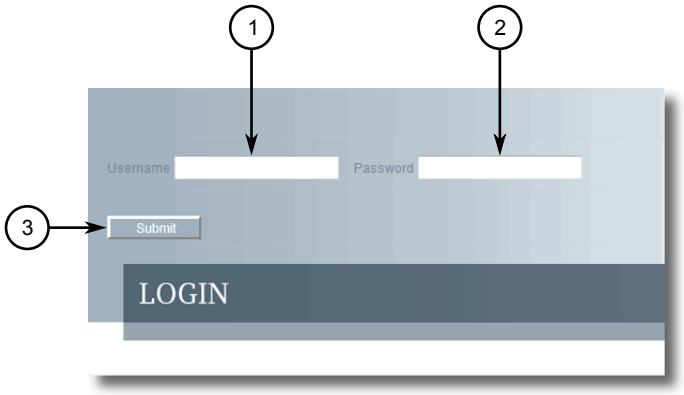


Figure 2: Login Screen (Web Interface)

1. Username Box **2.** Password Box **3.** Submit Button

NOTE

The following default usernames and passwords are set on the device for each user type:

Guest	***Operator***	***Admin***
Username: guest	*Username: operator*	*Username: admin*
Password: guest	*Password: operator*	*Password: admin*

CAUTION!
To prevent unauthorized access to the device, make sure to change the default guest, operator, and admin passwords before commissioning the device.

For more information about changing passwords, refer to Section 4.3, "Configuring Passwords".

2. In the **User Name** field, type the username for an account setup on the device.
3. In the **Password** field, typ the password for the account.
4. Click **Enter** or click **Submit** (Web interface only).

Section 2.3
Logging Out

To log out of the device, navigate to the main screen and do the following:

- To log out of the Console or secure shell interfaces, press **CTRL** + **X**.
- To log out of the Web interface, click **Logout**.

Figure 3: Web Interface (Example)

1. Logout

NOTE
If any pending configuration changes have not been committed, ROS will request confirmation before discarding the changes and logging out of the device.

Section 2.4
Using the Web Interface

The Web interface is a Web-based Graphical User Interface (GUI) for displaying important information and controls in a Web browser. The interface is divided into three frames: the banner, the menu and the main frame.

Figure 4: Web Interface Layout (Example)

1. Top Frame **2.** Side Frame **3.** Main Frame

Frame	Description
Top	The top frame displays the system name for the device.
Side	The side frame contains a logout option and a collapsible list of links that open various screens in the main frame. For information about logging out of ROS, refer to Section 2.3, “Logging Out”.
Main	The main frame displays the parameters and/or data related to the selected feature.

Each screen consists of a title, the current user's access level, parameters and/or data (in form or table format), and controls (e.g. add, delete, refresh, etc.). The title provides access to context-specific Help for the screen that provides important information about the available parameters and/or data. Click on the link to open the Help information in a new window.

When an alarm is generated, an alarm notification replaces the current user's access level on each screen until the alarm is cleared. The notification indicates how many alarms are currently active. For more information about alarms, refer to Section 4.4, “Managing Alarms”.

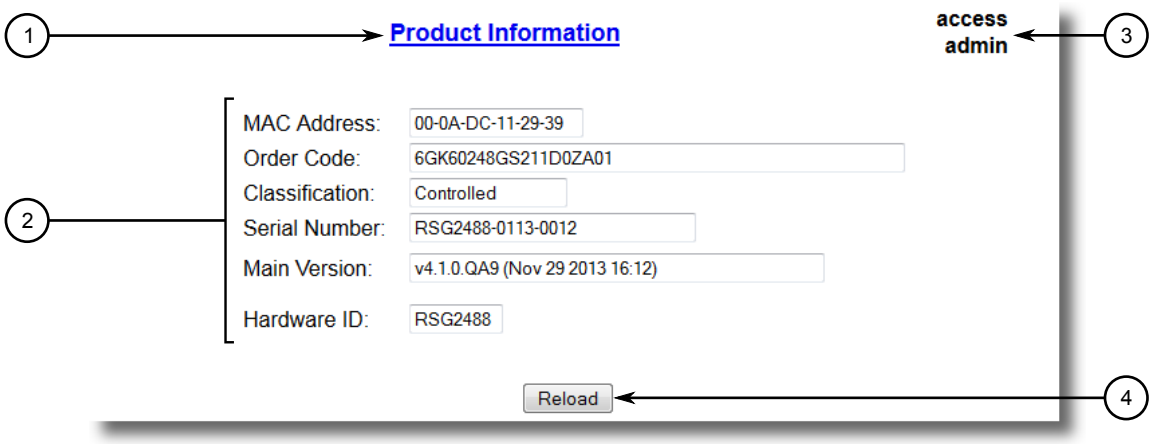


Figure 5: Elements of a Typical Screen (Example)

1. Title **2.** Parameters and/or Data **3.** Access Level or Alarm Notification **4.** Controls

Section 2.5

Using the Console Interface

The Console interface is a Graphical User Interface (GUI) organized as a series of menus. It is primarily accessible through a serial console connection, but can also be accessed through IP services, such as a Telnet, RSH (Remote Shell), or SSH (Secure Shell) session.

NOTE

IP services can be restricted to control access to the device. For more information, refer to Section 3.8, "Configuring IP Services".

Each screen consists of a system identifier, the name of the current menu, and a command bar. Alarms are also indicated on each screen in the upper right corner.

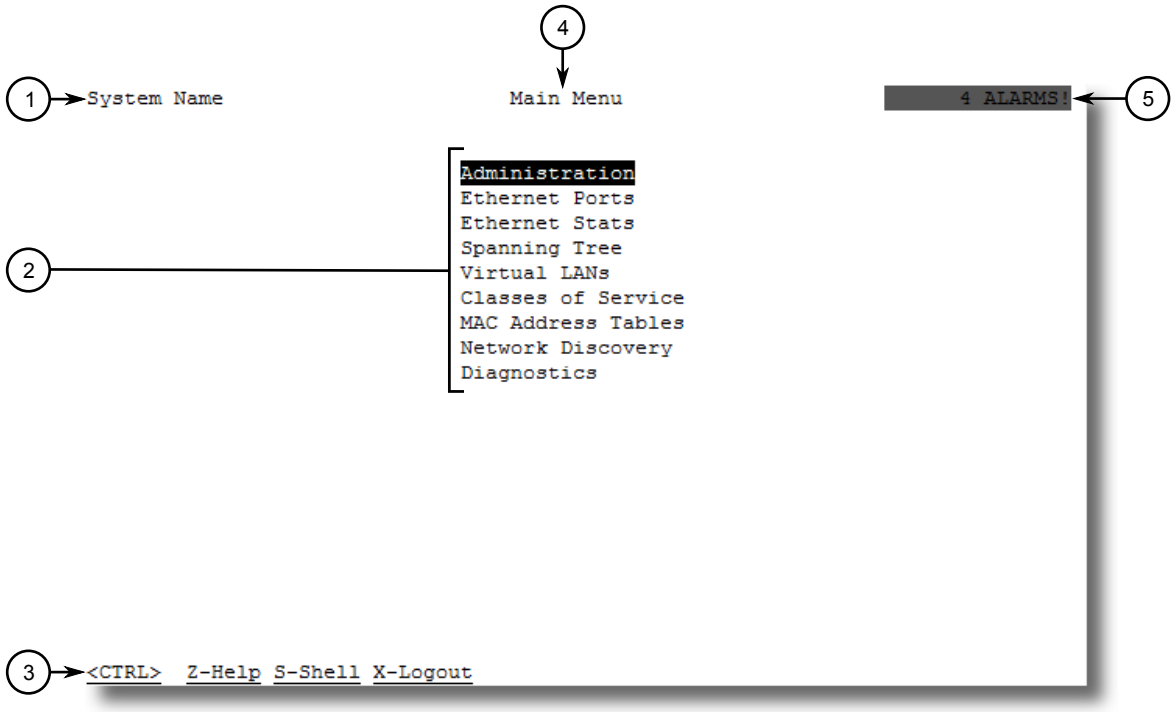


Figure 6: Console Interface (Example)

1. System Identification **2.** Menus **3.** Command Bar **4.** Menu Name **5.** Alarms Indicator

NOTE

They system identifier is user configurable. For more information about setting the system name, refer to Section 4.1, "Configuring the System Information".

Navigating the Interface

Use the following controls to navigate between screens in the Console interface:

Enter	Select a menu item and press this **Enter** to enter the sub-menu or screen beneath.
Esc	Press **Esc** to return to the previous screen.

Configuring Parameters

Use the following controls to select and configure parameters in the Console interface:

Up/Down Arrow Keys	Use the up and down arrow keys to select parameters.
Enter	Select a parameter and press **Enter** to start editing a parameter. Press **Enter** again to commit the change.
Esc	When editing a parameter, press **Esc** to abort all changes.

Commands

The command bar lists the various commands that can be issued in the Console interface. Some commands are specific to select screens. The standard commands include the following:

Ctrl + A	Commits configuration changes made on the current screen.

	NOTE *Before exiting a screen, ROS will automatically prompt the user to save any changes that have not been committed.*
Ctrl + I	Inserts a new record.
Ctrl + L	Deletes a record.
Ctrl + S	Opens the CLI interface.
Ctrl + X	Terminates the current session. This command is only available from the main menu.
Ctrl + Z	Displays important information about the current screen or selected parameter.

Section 2.6
Using the Command Line Interface

The Command Line Interface (CLI) offers a series of powerful commands for updating ROS, generating certificates/keys, tracing events, troubleshooting and much more. It is accessed via the Console interface by pressing **Ctrl-S**.

The following sections describe how to use the Command Line Interface (CLI):

- Section 2.6.1, “Available CLI Commands”
- Section 2.6.2, “Tracing Events”
- Section 2.6.3, “Executing Commands Remotely via RSH”
- Section 2.6.4, “Using SQL Commands”

Section 2.6.1
Available CLI Commands

The following commands are available at the command line:

Command	Description
alarms `all`	Displays a list of available alarms. Optional and/or required parameters include: • `all` displays all available alarms
arp	Displays the IP to MAC address resolution table.
clearalarms	Clears all alarms.
clearethstats `[all | port]`	Clears Ethernet statistics for one or more ports. Optional and/or required parameters include: • `all` clears statistics for all ports • *`port`* is a comma separated list of port numbers (e.g. 1,3-5,7)
clearlogs	Clears the system and crash logs.
clrcblstats `[all | port]`	Clears cable diagnostics statistics for one or more ports. Optional and/or required parameters include: • `all` clears statistics for all ports

Command	Description
	• *port* is a comma separated list of port numbers (e.g. 1,3-5,7)
clrstpstats	Clears all spanning tree statistics.
cls	Clears the screen.
dir	Prints the directory listing.
exit	Terminates the session.
factory	Enables factory mode, which includes several factory-level commands used for testing and troubleshooting. Only available to admin users. **CAUTION!** *Misuse of the factory commands may corrupt the operational state of device and/or may permanently damage the ability to recover the device without manufacturer intervention.*
flashfiles {info *filename* | defrag}	A set of diagnostic commands to display information about the Flash filesystem and to defragment Flash memory. Optional and/or required parameters include: • info *filename* displays information about the specified file in the Flash file system • defrag defragments files in the Flash file system For more information about the **flashfiles** command, refer to Section 2.8, "Managing the Flash File System".
flashleds *timeout*	Flashes the LED indicators on the device for a specified number of seconds. Optional and/or required parameters include: • *timeout* is the number of seconds to flash the LED indicators. To stop the LEDs from flashing, set the timeout period to 0 (zero).
fpgacmd	Provides access to the FPGA management tool for troubleshooting time synchronization.
help *command*	Displays a brief description of the specified command. If no command is specified, it displays a list of all available commands, including a description for each. Optional and/or required parameters include: • *command* is the command
ipconfig	Displays the current IP address, subnet mask and default gateway. This command provides the only way of determining these values when DHCP is used.
loaddflts	Loads the factory default configuration.
login	Logs in to the shell.
logout	Logs out of the shell.
ping *address* {*count* | *timeout*}	Sends an ICMP echo request to a remotely connected device. For each reply received, the round trip time is displayed. Use this command to verify connectivity to the next connected device. It is a useful tool for testing commissioned links. This command also includes the ability to send a specific number of pings with a specified time for which to wait for a response. Optional and/or required parameters include: • *address* is the target IP address. • *count* is the number of echo requests to send. The default is 4. • *timeout* is the time in milliseconds to wait for each reply. The range is 2 to 5000 seconds. The default is 300 milliseconds. **NOTE** *The device to be pinged must support ICMP echo. Upon commencing the ping, an ARP request for the MAC address of the device is issued. If the device to be*

Command	Description
	pinged is not on the same network as the device pinging the other device, the default gateway must be programmed.
purgemac	Purges the MAC Addrtess table.
reset	Perform a hard reset of the switch.
resetport {all | *ports*}	Resets one or more Ethernet ports, which may be useful for forcing re-negotiation of speed and duplex, or in situations where the link partner has latched into an inappropriate state. Optional and/or required parameters include: • all resets all ports • *ports* is a comma separated list of port numbers (e.g. 1,3-5,7)
rmon	Displays the names of all RMON alarm eligible objects.
route	Displays the gateway configuration.
sfp *port* {base | alarms | diag | calibr | thr | all | no parameter specified}	Displays SFP (Small Form Factor Pluggable) device information and diagnostics. If optional or required parameters are not used, this command displays the base and extended information. Optional and/or required parameters include: • *port* is the port number for which the data are required • base displays the base information • alarms displays alarms and warning flags • diag displays measured data • calibr displays calibration data for external calibration • thr displays thresholds data • all displays all diagnostic data
sql {default | delete | help | info | insert | save | select | update}	Provides an SQL-like interface for manipulating all system configuration and status parameters. All commands, clauses, table, and column names are case insensitive. Optional and/or required parameters include: • default sets all records in a table(s) to factory defaults • delete allows for records to be deleted from a table • help provides a brief description for any SQL command or clause • info displays a variety of information about the tables in the database • insert enables new records to be inserted into a table • save saves the database to non-volatile memory storage • select queries the dtabase and displays selected records • update enable existing records in a table to be updated For more information about the **sql** command, refer to Section 2.6.4, “Using SQL Commands”.
sshkeygen *size*	Generates new SSH keys in ssh.keys. Optional and/or required parameters include: • *size* is the number of bits in length between 512 and 2048. The default is 1024 bits.
sslkeygen *size*	Generates a new SSL certificate in ssl.crt. Optional and/or required parameters include: • *size* is the number of bits in length between 512 and 2048. The default is 1024 bits.
telnet *dest*	Opens a telnet session. Press **Ctrl-C** to close the session. Optional and/or required parameters include: • *dest* is the server's IP address
tftp {*dest* | *cmd* | *fsource* | *fdest*}	Opens a TFTP session. Press **Ctrl-C** to close the session.

Command	Description
	Optional and/or required parameters include: • *dest* is the remote TFTP server's IP address • *cmd* is either **put** (upload) or **get** (download) • *fsource* is the source filename • *fdest* is the destination filename
trace	Starts event tracing. Run **trace ?** for more help.
type *filename*	Displays the contents of a text file. Optional and/or required parameters include: • *filename* is the name of the file to be read
version	Prints the software version.
xmodem {send | receive} *filename*	Opens an XModem session. Optional and/or required parameters include: • send sends the file to the client. • receive receives the file from the client. • *filename* is the name of the file to be read.

Section 2.6.2
Tracing Events

The CLI trace command provides a means to trace the operation of various protocols supported by the device. Trace provides detailed information, including STP packet decodes and MAC address displays.

NOTE
Tracing has been designed to provide detailed information to expert users. Note that all tracing is disabled upon device startup.

To trace an event, do the following:

1. Log in to the device as an admin user and access the CLI shell. For more information about accessing the CLI shell, refer to Section 2.6, “Using the Command Line Interface”.
2. Determine the protocols and associated options available by typing:

   ```
   trace ?
   ```

   If an option such as allon or alloff is required, determine which options are available for the desired protocol by typing:

   ```
   trace protocol ?
   ```

   NOTE
   If required, expand the trace scope by stringing protocols and their associated options together using a vertical bar (|).

3. Select the type of trace to run by typing:

   ```
   trace protocol option
   ```

   Where:

   • *protocol* is the protocol to trace

- *option* is the option to use during the trace

Example:

```
>trace transport allon
                      TRANSPORT: Logging is enabled
```

4. Start the trace by typing:

```
trace
```

Section 2.6.3

Executing Commands Remotely via RSH

The Remote Shell (RSH) facility can be used from a workstation to cause the product to act upon commands as if they were entered at the CLI prompt. The syntax of the RSH command is usually of the form:

```
rsh ipaddr -l auth_token command_string
```

Where:

- *ipaddr* is the address or resolved name of the device.
- *auth_token* is the user name (i.e. guest, operator or admin) and corresponding password separated by a comma. For example, *admin,secret*.
- *command_string* is the ROS CLI command to execute.

NOTE
The access level (corresponding to the user name) selected must support the given command.

NOTE
Any output from the command will be returned to the workstation submitting the command. Commands that start interactive dialogs (such as **trace***) cannot be used.*

Section 2.6.4

Using SQL Commands

ROS provides an *SQL-like* command facility that allows expert users to perform several operations not possible under the traditional Web or CLI interface. For instance:

- Restoring the contents of a specific table, but not the whole configuration, to their factory defaults.
- Search tables in the database for specific configurations.
- Make changes to tables predicated upon existing configurations.

When combined with RSH, SQL commands provide a means to query and configure large numbers of devices from a central location.

NOTE
For a list of parameters available under the **sql** *command, refer to* *Section 2.6.1, "Available CLI Commands"**.*

The following sections describe in more detail how to use SQL commands:

- Section 2.6.4.1, “Finding the Correct Table”
- Section 2.6.4.2, “Retrieving Information”
- Section 2.6.4.3, “Changing Values in a Table”
- Section 2.6.4.4, “Resetting a Table”
- Section 2.6.4.5, “Using RSH and SQL”

Section 2.6.4.1

Finding the Correct Table

Many SQL commands operate upon specific tables in the database, and require the table name to be specified. Navigating the menu system in the console interface to the desired menu and pressing **Ctrl-Z** displays the name of the table. The menu name and the corresponding database table name will be cited.

Another way to find a table name is to type the following in the CLI:

```
sql info tables
```

This command also displays menu names and their corresponding database table names depending upon the features supported by the device. For example:

```
Table Description
-------------------------------------------------------------------------------
alarms Alarms
cpuDiags CPU Diagnostics
ethPortCfg Port Parameters
ethPortStats Ethernet Statistics
ethPortStatus Port Status
ipCfg IP Services
```

Section 2.6.4.2

Retrieving Information

The following describes various methods for retrieving information about tables and parameters.

Retrieving Information from a Table

Use the following command to display a summary of the parameters within a table, as well as their values:

```
sql select from table
```

Where:

- *table* is the name of the table

Example:

```
>sql select from ipAddrtable

IP Address      Subnet          IfIndex    IfStats    IfTime     IfName
172.30.146.88   255.255.224.0   1001       17007888   2994       vlan1

1 records selected
```

Retrieving Information About a Parameter from a Table

Use the following command to retrieve information about a specific parameter from a table:

NOTE
The parameter name must be the same as it is displayed in the menu system, unless the name contains spaces (e.g. ip address). Spaces must be replaced with underscores (e.g. ip_address) or the parameter name must be wrapped in double quotes (e.g. "ip address").

```
sql select parameter from table
```

Where:

- *parameter* is the name of the parameter
- *table* is the name of the table

Example:

```
>sql select "ip address" from ipSwitchIfCfg

IP Address
192.168.0.1

1 records selected
```

Retrieving Information from a Table Using the *Where* Clause

Use the following command to display specific parameters from a table that have a specific value:

```
sql select from table where parameter = value
```

Where:

- *table* is the name of the table
- *parameter* is the name of the parameter
- *value* is the value of the parameter

Example:

```
>sql select from ethportcfg where media = 1000T

Port Name            ifName          Media       State    AutoN Speed Dupx  FlowCtrl LFI Alarm
1  Port 1          1             1000T       Enabled  On    Auto  Auto  Off      Off On
2  Port 2          2             1000T       Enabled  On    Auto  Auto  Off      Off On
3  Port 3          3             1000T       Enabled  On    Auto  Auto  Off      Off On
4  Port 4          4             1000T       Enabled  On    Auto  Auto  Off      Off On

4 records selected
```

Further refine the results by using `and` or `or` operators:

```
sql select from table where parameter = value [{and | or} | parameter | = | value...]
```

Where:

- *table* is the name of the table
- *parameter* is the name of the parameter
- *value* is the value of the parameter

Example:

```
>sql select from ethportcfg where media = 1000T and State = enabled
```

```
Port Name             ifName          Media       State    AutoN Speed Dupx  FlowCtrl LFI Alarm
1  Port 1          1             1000T       Enabled  On    Auto  Auto  Off      Off on
2  Port 2          2             1000T       Enabled  On    Auto  Auto  Off      Off On
3  Port 3          3             1000T       Enabled  On    Auto  Auto  Off      Off On
4  Port 4          4             1000T       Enabled  On    Auto  Auto  Off      Off On

4 records selected
```

Section 2.6.4.3

Changing Values in a Table

Use the following command to change the value of parameters in a table:

```
sql update table set parameter = value
```

Where:

- *table* is the name of the table
- *parameter* is the name of the parameter
- *value* is the value of the parameter

Example:

```
>sql update iplcfg set IP_Address_Type = static
1 records updated
```

Conditions can also be included in the command to apply changes only to parameters that meet specific criteria. In the following example, flow control is enabled on ports that are operating in 100 Mbps full-duplex mode with flow control disabled:

```
>sql update ethportcfg set FlowCtrl = Off where ( Media = 100TX and FlowCtrl = On )
2 records updated
```

Section 2.6.4.4

Resetting a Table

Use the following command to reset a table back to its factory defaults:

```
sql default into table
```

Where:

- *table* is the name of the table

Section 2.6.4.5

Using RSH and SQL

The combination of remote shell scripting and SQL commands offers a means to interrogate and maintain a large number of devices. Consistency of configuration across sites may be verified by this method. The following presents a simple example where the devices to interrogate are drawn from the file `Devices`:

Need a new example not related to VLANs

```
C:> type Devices
```

```
10.0.1.1
10.0.1.2

C:\> for /F %i in (devices) do rsh %i -l admin,admin sql select from ipAddrtable

C:\>rsh 10.0.1.1 -l admin,admin sql select from ipAddrtable

IP Address      Subnet          IfIndex    IfStats    IfTime     IfName
192.168.0.31    255.255.255.0   1001       274409096  2218       vlan1

1 records selected

C:\>rsh 10.0.1.2 -l admin,admin sql select from ipAddrtable
0 records selected
C:\
```

Section 2.7

Selecting Ports in ROS

Many features in ROS can be configured for one or more ports on the device. The following describes how to specify a single port, a range of ports, or all ports.

Select a single port by specifying the port number:

```
2
```

Select a range of ports using a dash (-) between the first port and the last port in the list:

```
1-4
```

Select multiple ports by defining a comma-separated list:

```
1,4,6,9
```

Use the *All* option to select all ports in the device, or, if available, use the *None* option to select none of the ports.

Section 2.8

Managing the Flash File System

The following sections describe how to manage the flash file system:

- Section 2.8.1, “Viewing a List of Flash Files”
- Section 2.8.2, “Viewing Flash File Details”
- Section 2.8.3, “Defragmenting the Flash File System”

Section 2.8.1

Viewing a List of Flash Files

To view a list of files currently stored in Flash memory, do the following:

1. Log in to the device as an admin user and access the CLI shell. For more information about accessing the CLI shell, refer to Section 2.6, “Using the Command Line Interface”.
2. Type **`flashfiles`**. A list of files currently in Flash memory is displayed, along with their locations and the amount of memory they consume. For example:

```
>flashfiles
------------------------------------------------------------------
Filename             Base    Size  Sectors     Used
------------------------------------------------------------------
boot.bin         00000000 110000    0-16   1095790
main.bin         00110000 140000   17-36   1258403
fpga.xsvf        00250000 010000   37-37     55882
syslog.txt       00260000 140000   38-57     19222
ssh.keys         003A0000 010000   58-58       915
ssl.crt          003B0000 010000   59-59      1970
banner.txt       003C0000 010000   60-60       256
crashlog.txt     003D0000 010000   61-61       256
config.bak       003E0000 010000   62-62     15529
config.csv       003F0000 008000   63-63     15529
factory.txt      003FC000 004000   66-66       407
------------------------------------------------------------------
```

Section 2.8.2
Viewing Flash File Details

To view the details of a file currently stored in Flash memory, do the following:

1. Log in to the device as an admin user and access the CLI shell. For more information about accessing the CLI shell, refer to Section 2.6, “Using the Command Line Interface”.
2. Display information about a file by typing:

```
flashfiles info filename
```

Where:

- *`filename`* is the name of the file stored in Flash memory

Details, similar to the following, are displayed.

Updated for RP110

```
>flashfiles info main.bin

Flash file information for main.bin:
Header version   : 4
Platform         : ROS-CF52

File name        : main.bin
Firmware version : v4.1.0
Build date       : Sep 27 2014 15:50
File length      : 2624659
Board IDs        :  3d
Header CRC       : 73b4
Header CRC Calc  : 73b4
Body CRC         : b441
Body CRC Calc    : b441
```

Section 2.8.3

Defragmenting the Flash File System

The flash memory is defragmented automatically whenever there is not enough memory available for a binary upgrade. However, fragmentation can occur whenever a new file is uploaded to the unit. Fragmentation causes sectors of available memory to become separated by ones allocated to files. In some cases, the total available memory might be sufficient for a binary upgrade, but that memory may not be available in one contiguous region.

To defragment the flash memory, do the following:

1. Log in to the device as an admin user and access the CLI shell. For more information about accessing the CLI shell, refer to Section 2.6, “Using the Command Line Interface”.
2. Defragment the flash memory by typing:

```
flashfiles defrag
```

Section 2.9

Accessing BIST Mode

BIST (Built-In-Self-Test) mode is used by service technicians to test and configure internal functions of the device. It should only be accessed for troubleshooting purposes.

CAUTION!
Mechanical hazard – risk of damage to the device. Excessive use of BIST functions may cause increase wear on the device, which may void the warranty. Avoid using BIST functions unless instructed by a Siemens Customer Support representative.

To access BIST mode, do the following:

IMPORTANT!
Do not connect the device to the network when it is in BIST mode. The device will generate excess multicast traffic in this mode.

1. Disconnect the device from the network.
2. Connect to ROS through the RS232 console connection and a terminal application. For more information, refer to Section 2.1.1, “Connecting Directly”.
3. Reset the device. For more information, refer to Section 3.11, “Resetting the Device”.
4. During the boot up sequence, press **Ctrl-C** when prompted. The command prompt for BIST appears.

```
>
```

5. Type **`help`** to view a list of all available options under BIST.

3 Device Management

This chapter describes how to configure and manage the device and its components, such as module interfaces, logs and files. It describes the following tasks:

NOTE
For information about how to configure the device to work with a network, refer to Chapter 5, Setup and Configuration.

- Section 3.1, “Viewing Product Information”
- Section 3.2, “Viewing CPU Diagnostics”
- Section 3.3, “Restoring Factory Defaults”
- Section 3.4, “Configuring an IP Interface”
- Section 3.5, “Uploading/Downloading Files”
- Section 3.6, “Managing Logs”
- Section 3.7, “Managing IP Gateways”
- Section 3.8, “Configuring IP Services”
- Section 3.9, “Managing Remote Monitoring”
- Section 3.10, “Upgrading/Downgrading Firmware”
- Section 3.11, “Resetting the Device”
- Section 3.12, “Decommissioning the Device”

Section 3.1
Viewing Product Information

During troubleshooting or when ordering new devices, Siemens personnel may request specific information about the device, such as the model, order code or serial number.

To view information about the device, navigate to ***Diagnostics*** » ***View Product Information***. The **Product Information** form appears.

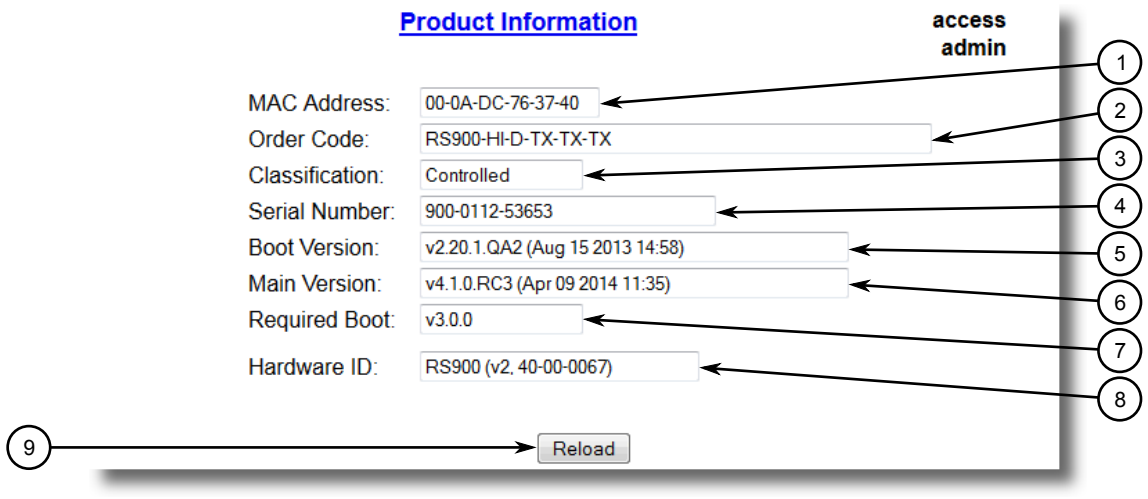


Figure 7: Product Information Form (Example)

1. MAC Address Box **2.** Order Code Box **3.** Classification Box **4.** Serial Number Box **5.** Boot Version Box **6.** Main Version Box **7.** Required Boot Box **8.** Hardware ID Box **9.** Reload Button

This screen displays the following information:

Parameter	Description
MAC Address	**Synopsis:** ##-##-##-##-##-## where ## ranges 0 to FF Shows the unique MAC address of the device.
Order Code	**Synopsis:** Any 57 characters Shows the order code of the device.
Classification	**Synopsis:** Any 15 characters Provides system classification. The value *Controlled* indicates the main firmware is a Controlled release. The value *Non-Controlled* indicates the main firmware is a Non-Controlled release. The *Controlled* main firmware can run on Controlled units, but it can not run on Non-Controlled units. The *Non-Controlled* main firmware can run on both Controlled and Non-Controlled units.
Serial Number	**Synopsis:** Any 31 characters Shows the serial number of the device.
Boot Version	**Synopsis:** Any 47 characters Shows the version and the build date of the boot loader software.
Main Version	**Synopsis:** Any 47 characters Shows the version and build date of the main operating system software.
Required Boot	**Synopsis:** Any 15 characters Shows the minimum boot software loader version required by running main.
Hardware ID	**Synopsis:** { RSMCPU (40-00-0008 Rev B1), RSMCPU2 (40-00-0026 Rev A1), RS400 (40-00-0010 Rev B2), RMC30, RS900 (40-00-0025 Rev B1), RS900 (40-00-0032 Rev B1), RS1600M, RS400 (40-00-0010 Rev C1), RSG2100, RS900G, RSG2200, RS969, RS900 (v2, 40-00-0066), RS900 (v2, 40-00-0067), , RS416 (40-00-0078), RMC30 (v2), RS930 (40-00-0089), RS969 (v2, 40-00-0090), RS910 (40-00-0091-001 Rev A), RS920L (40-00-0102-001 Rev A), RS940G (40-00-0097-000 Rev A), RSi80X series CPU board, RSG2300, RS416v2, ... }

Parameter	Description
	Shows the type, part number, and revision level of the hardware.

Section 3.2

Viewing CPU Diagnostics

To view CPU diagnostic information useful for troubleshooting hardware and software performance, navigate to ***Diagnostics » View CPU Diagnostics***. The **CPU Diagnostics** form appears.

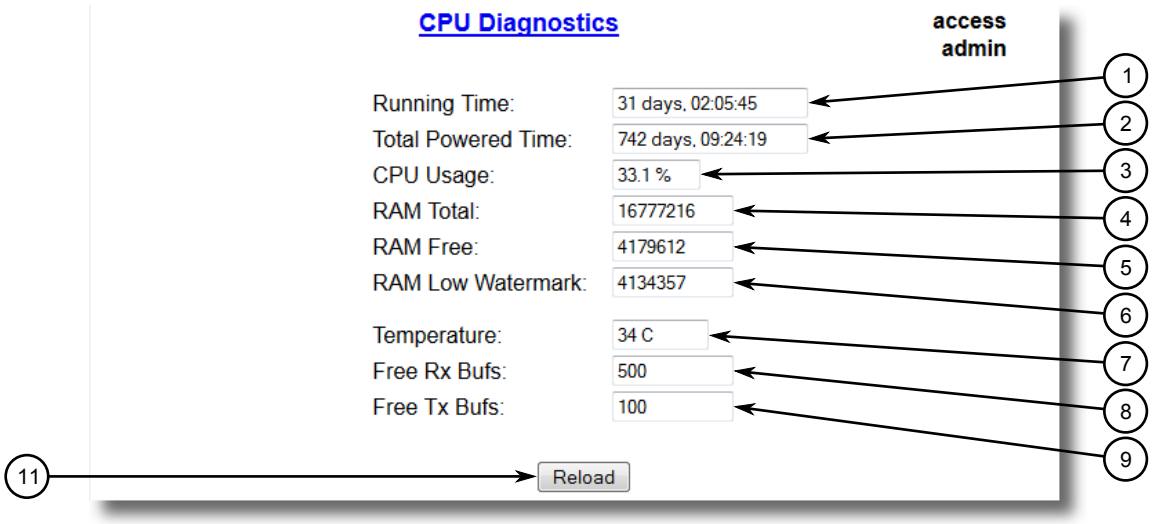


Figure 8: CPU Diagnostics Form

1. Running Time Box **2.** Total Powered Time Box **3.** CPU Usage Box **4.** RAM Total Box **5.** RAM Free Box **6.** RAM Low Watermark Box **7.** Temperature Box **8.** Free Rx Bufs Box **9.** Free Tx Bufs Box **10.** Reload Button

This screen displays the following information:

Parameter	Description
Running Time	**Synopsis:** DDDD days, HH:MM:SS The amount of time since the device was last powered on.
Total Powered time	**Synopsis:** DDDD days, HH:MM:SS The cumulative powered up time of the device.
CPU Usage	**Synopsis:** 0.0 to 100.0% The percentage of available CPU cycles used for device operation as measured over the last second.
RAM Total	**Synopsis:** 0 to 4294967295 The total size of RAM in the system.
RAM Free	**Synopsis:** 0 to 4294967295 The total size of RAM still available.
RAM Low Watermark	**Synopsis:** 0 to 4294967295

Parameter	Description
	The size of RAM that have never been used during the system runtime.
Temperature	**Synopsis:** -32768 to 32767 C The temperature on CPU board.
Free Rx Bufs	**Synopsis:** 0 to 4294967295 Free Rx Buffers.
Free Tx Bufs	**Synopsis:** 0 to 4294967295 Free Tx Buffers.

Section 3.3

Restoring Factory Defaults

The device can be completely or partially restored to its original factory default settings. Excluding groups of parameters from the factory reset, such as those that affect basic connectivity and SNMP management, is useful when communication with the device is still required during the reset.

The following categories are not affected by a selective configuration reset:

- IP Interfaces
- IP Gateways
- SNMP Users
- SNMP Security to Group Maps
- SNMP Access

In addition, the following categories are not affected by a full or selective configuration reset:

- Time Zone
- DST Offset
- DST Rule

To restore factory defaults, do the following:

1. Navigate to ***Diagnostics*** » ***Load Factory Defaults***. The **Load Factory Defaults** form appears.

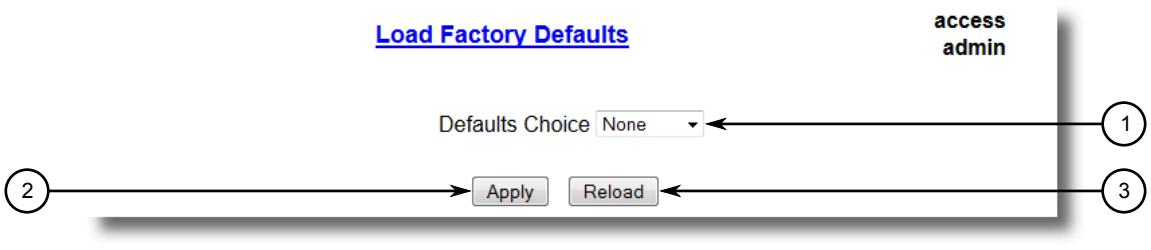


Figure 9: Load Factory Defaults Form

1. Defaults Choice List **2.** Apply Button **3.** Reload

2. Configure the following parameter(s) as required:

Parameter	Description
Defaults Choice	**Synopsis:** { None, Selected, All } Setting some records like IP Interfaces management interface, default gateway, SNMP settings to default value would cause switch not to be accessible with management applications. This parameter allows user to choose to load defaults to Selected tables, which would preserve configuration for tables that are critical for switch management applications, or to force All tables to default settings.

3. Click **Apply**.

Section 3.4
Configuring an IP Interface

To configure the IP interface, do the following:

1. Navigate to ***Administration*** » ***Configure IP Interfaces***. The **IP Interfaces** form appears.

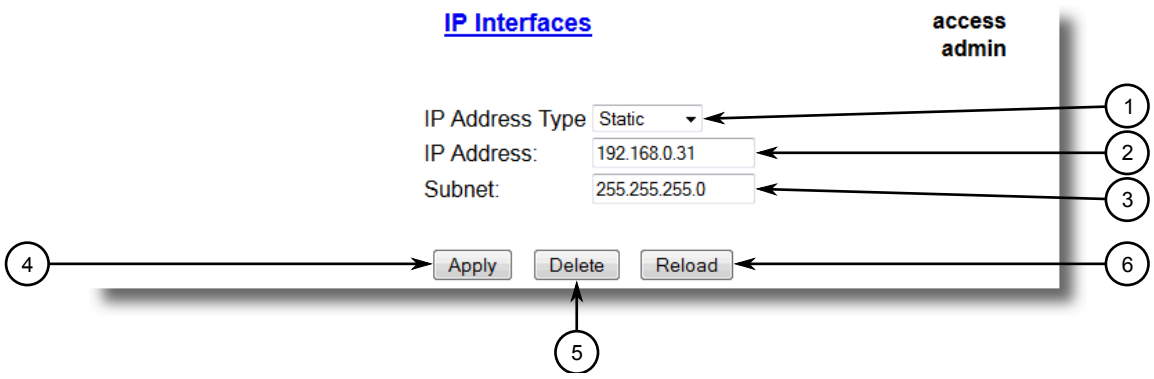


Figure 10: IP Interfaces Form

1. IP Address Type Box **2.** IP Address Box **3.** Subnet Box **4.** Apply Button **5.** Delete Button **6.** Reload Button

2. Configure the following parameter(s) as required:
3. Click **Apply**.

Section 3.5
Uploading/Downloading Files

Files can be transferred between the device and a host computer using any of the following methods:

- Xmodem using the CLI shell over a Telnet or RS232 console session
- TFTP client using the CLI shell in a console session and a remote TFTP server
- TFTP server from a remote TFTP client
- SFTP (secure FTP over SSH) from a remote SFTP client

NOTE
The contents of the internal file system are fixed. New files and directories cannot be created, and existing files cannot be deleted. Only the files that can be uploaded to the device can be overwritten.

Files that may need to be uploaded or downloaded include:

- `main.bin` – the main ROS application firmware image
- `boot.bin` – the boot loader firmware image
- `fpga.xsvf` – the FPGA firmware binary image
- `config.csv` – the complete configuration database, in the form of a comma-delimited ASCII text file
- `banner.txt` – contains text that appears on the login screen

The following sections describe how to upload and download files:

- Section 3.5.1, “Uploading/Downloading Files Using XMODEM”
- Section 3.5.2, “Uploading/Downloading Files Using a TFTP Client”
- Section 3.5.3, “Uploading/Downloading Files Using a TFTP Server”
- Section 3.5.4, “Uploading/Downloading Files Using an SFTP Server”

Section 3.5.1
Uploading/Downloading Files Using XMODEM

To updload or download a file using XMODEM, do the following:

NOTE
This method requires a host computer that has terminal emulation or Telnet software installed and the ability to perform XMODEM transfers.

NOTE
Xmodem transfers can only be performed through the serial console, which is authenticated during login.

1. Establish a direct connection between the device and the host computer. For more information, refer to Section 2.1.1, “Connecting Directly”.
2. Log in to the device as an admin user and access the CLI shell. For more information about accessing the CLI shell, refer to Section 2.6, “Using the Command Line Interface”.

   NOTE
   The `send` *option sends files to the host computer, while the* `receive` *option pulls files from the host computer.*

3. At the CLI prompt, type:

   ```
   xmodem [send | receive] filename
   ```

   Where:

   - *`filename`* is the name of the file (i.e. main.bin)

NOTE
If available in the terminal emulation or Telnet software, select the XModem 1K protocol for transmission over the standard XModem option.

4. When the device responds with

```
Press Ctrl-X to cancel
```

, launch the XMODEM transfer from the host computer. The device will indicate when the transfer is complete.

The following is an example from the CLI shell of a successful XMODEM file transfer:

```
>xmodem receive main.bin
Press Ctrl-X to cancel
Receiving data now ...C
Received 1428480 bytes. Closing file main.bin ...
main.bin transferred successfully
```

Section 3.5.2

Uploading/Downloading Files Using a TFTP Client

To updload or download a file using a TFTP client, do the following:

IMPORTANT!
TFTP does not define an authentication scheme. Any use of the TFTP client or server is considered highly insecure.

NOTE
This method requires a TFTP server that is accessible over the network.

1. Identify the IP address of the computer running the TFTP server.
2. Establish a direct connection between the device and a host computer. For more information, refer to Section 2.1.1, “Connecting Directly”.
3. Log in to the device as an admin user and access the CLI shell. For more information about accessing the CLI shell, refer to Section 2.6, “Using the Command Line Interface”.
4. At the CLI prompt, type:

```
tftp address [get | put] source-filename destination-filename
```

Where:

- `get` copies files from the host computer to the device
- `put` copies files from the device to the host computer
- *`address`* is the IP address of the computer running the TFTP server
- *`source-filename`* is the name of the file to be transferred
- *`destination-filename`* is the name of the file (on the device or the TFTP server) that will be replaced during the transfer

The following is an example of a successful TFTP client file transfer:

```
>tftp 10.0.0.1 get ROS-CF52_Main_v3.7.0.bin main.bin
TFTP CMD: main.bin transfer ok. Please wait, closing file ...
```

```
TFTP CMD: main.bin loading succesful.
```

Section 3.5.3

Uploading/Downloading Files Using a TFTP Server

To updload or download a file using a TFTP server, do the following:

IMPORTANT!
TFTP does not define an authentication scheme. Any use of the TFTP client or server is considered highly insecure.

NOTE
This method requires a host computer that has TFTP server software installed.

IMPORTANT!
Interaction with TFTP servers is strictly controlled within the device to prevent unauthorized access. Make sure the device is configured to accept the TFTP connection. For more information, refer to Section 3.8, "Configuring IP Services".

1. Establish a direct connection between the device and the host computer. For more information, refer to Section 2.1.1, "Connecting Directly".
2. Initialize the TFTP server on the host computer and launch the TFTP transfer. The server will indicate when the transfer is complete.

   The following is an example of a successful TFTP server exchange:

```
C:\>tftp -i 10.1.0.1 put C:\files\ROD-CF52_Main_v3.7.0.bin main.bin
Transfer successful: 1428480 bytes in 4 seconds, 375617 bytes/s
```

Section 3.5.4

Uploading/Downloading Files Using an SFTP Server

SFTP (Secure File Transfer Protocol) is a file transfer mechanism that uses SSH to encrypt every aspect of file transfer between a networked client and server.

NOTE
The device does not have an SFTP client and, therefore, can only receive SFTP files from an external source. SFTP requires authentication for the file transfer.

To updload or download a file using an SFTP server, do the following:

NOTE
This method requires a host computer that has SFTP client software installed.

1. Establish an SFTP connection between the device and the host computer.
2. Launch the SFTP transfer. The client will indicate when the transfer is complete.

   The following is an example of a successful SFTP server exchange:

```
user@host$ sftp admin@ros_ip
Connecting to ros_ip...
admin@ros_ip's password:
sftp> put ROS-CF52_Main_v3-7-0.bin main.bin
Uploading ROS-CF52_Main_v3-7-0.bin to /main.bin
ROS-CF52_Main_v3-7-0.bin 100% 2139KB 48.6KB/s 00:44
sftp>
```

Section 3.6

Managing Logs

The crash (`crashlog.txt`) and system (`syslog.txt`) log files contain historical information about events that have occurred during the operation of the device.

The crash log contains debugging information related to problems that might have resulted in unplanned restarts of the device or which may effect the operation of the device. A file size of 0 bytes indicates that no unexpected events have occurred.

The system log contains a record of significant events including startups, configuration changes, firmware upgrades and database re-initializations due to feature additions. The system log will accumulate information until it is full, holding approximately 2 MB of data.

The following sections describe how to configure and manage logs:

- Section 3.6.1, “Viewing Local Logs”
- Section 3.6.2, “Clearing Local Logs”
- Section 3.6.3, “Configuring the Local System Log”
- Section 3.6.4, “Managing Remote Logging”

Section 3.6.1

Viewing Local Logs

The local crash and system logs can both be downloaded from the device and viewed in a text editor. For more information about downloading log files, refer to Section 3.5, “Uploading/Downloading Files”.

To view the system log through the Web interface, navigate to ***Diagnostics*** » ***View System Log***. The **syslog.txt** form appears.

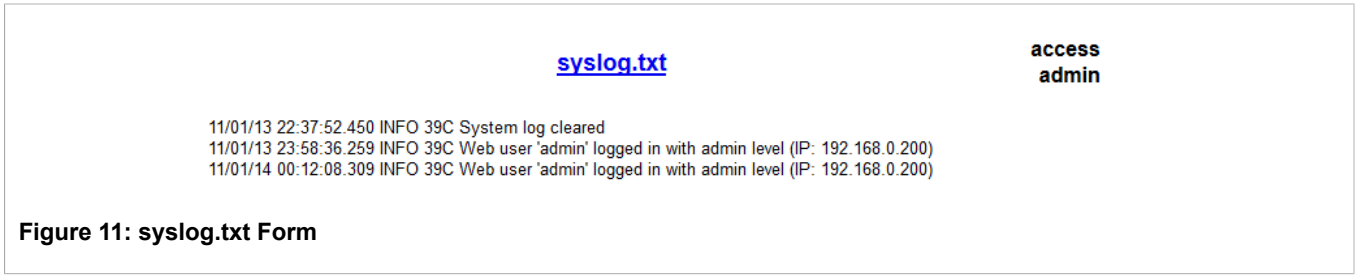

syslog.txt
access
admin
11/01/13 22:37:52.450 INFO 39C System log cleared
11/01/13 23:58:36.259 INFO 39C Web user 'admin' logged in with admin level (IP: 192.168.0.200)
11/01/14 00:12:08.309 INFO 39C Web user 'admin' logged in with admin level (IP: 192.168.0.200)

Figure 11: syslog.txt Form

Section 3.6.2
Clearing Local Logs

To clear both the local crash and system logs, log in to the CLI shell and type:

```
clearlogs
```

To clear only the local system log, log in to the Web interface and do the following:

1. Navigate to ***Diagnostics*** » ***Clear System Log***. The **Clear System Log** form appears.

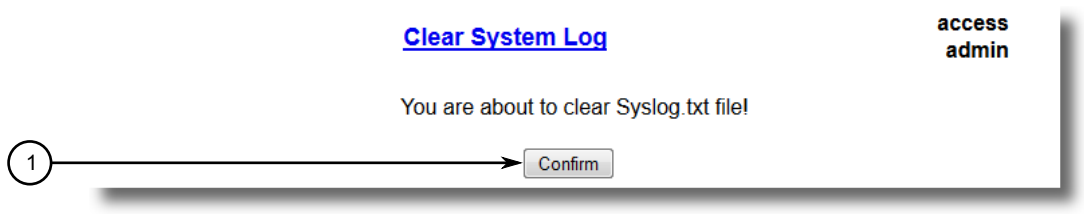


Figure 12: Clear System Log Form

1. Confirm Button

2. Click **Confirm**.

Section 3.6.3
Configuring the Local System Log

To configure the severity level for the local system log, do the following:

> **NOTE**
> *For maximum reliability, use remote logging. For more information, refer to Section 3.6.4, "Managing Remote Logging".*

1. Navigate to ***Administration*** » ***Configure Syslog*** » ***Configure Local Syslog***. The **Local Syslog** form appears.

Figure 13: Local Syslog Form

1. Local Syslog Level **2.** Apply Button **3.** Reload Button

2. Configure the following parameter(s) as required:

Parameter	Description
Local Syslog Level	**Synopsis:** { EMERGENCY, ALERT, CRITICAL, ERROR, WARNING, NOTICE, INFORMATIONAL, DEBUGGING } **Default:** INFORMATIONAL The severity of the message that has been generated. Note that the severity level selected is considered the minimum severity level for the system. For example, if ERROR is selected, the system sends any syslog messages generated by Error, Critical, Alert and Emergency.

3. Click **Apply**.

Section 3.6.4
Managing Remote Logging

In addition to the local system log maintained on the device, a remote system log can be configured as well to collect important event messages. The syslog client resides on the device and supports up to 5 collectors (or syslog servers).

The remote syslog protocol, defined in RFC 3164, is a UDP/IP-based transport that enables the device to send event notification messages across IP networks to event message collectors, also known as syslog servers. The protocol is designed to simply transport these event messages from the generating device to the collector(s).

The following sections describe how to configure a remote syslog client and server:

- Section 3.6.4.1, “Configuring the Remote Syslog Client”
- Section 3.6.4.2, “Viewing a List of Remote Syslog Servers”
- Section 3.6.4.3, “Adding a Remote Syslog Server”
- Section 3.6.4.4, “Deleting a Remote Syslog Server”

Section 3.6.4.1
Configuring the Remote Syslog Client

To configure the remote syslog client, do the following:

1. Navigate to ***Administration*** » ***Configure Syslog*** » ***Configure Remote Syslog Client***. The **Remote Syslog Client** form appears.

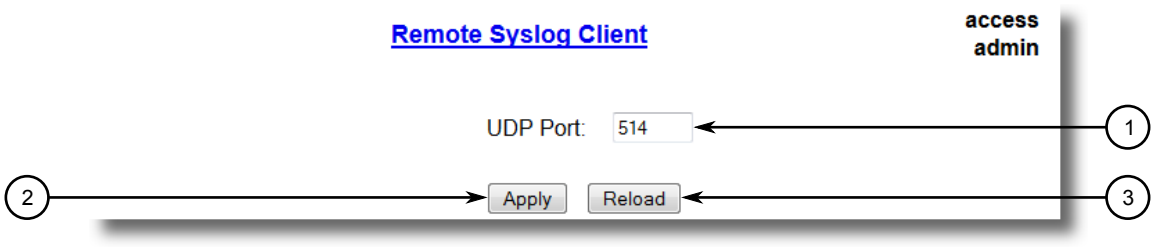


Figure 14: Remote Syslog Client Form

1. UDP Port **2.** Apply Button **3.** Reload Button

2. Configure the following parameter(s) as required:

Parameter	Description
UDP Port	**Synopsis:** 1025 to 65535 or { 514 } **Default:** 514 The local UDP port through which the client sends information to the server(s).

3. Click **Apply**.

Section 3.6.4.2
Viewing a List of Remote Syslog Servers

To view a list of known remote syslog servers, navigate to ***Administration » Configure Syslog » Configure Remote Syslog Server***. The **Remote Syslog Server** table appears.

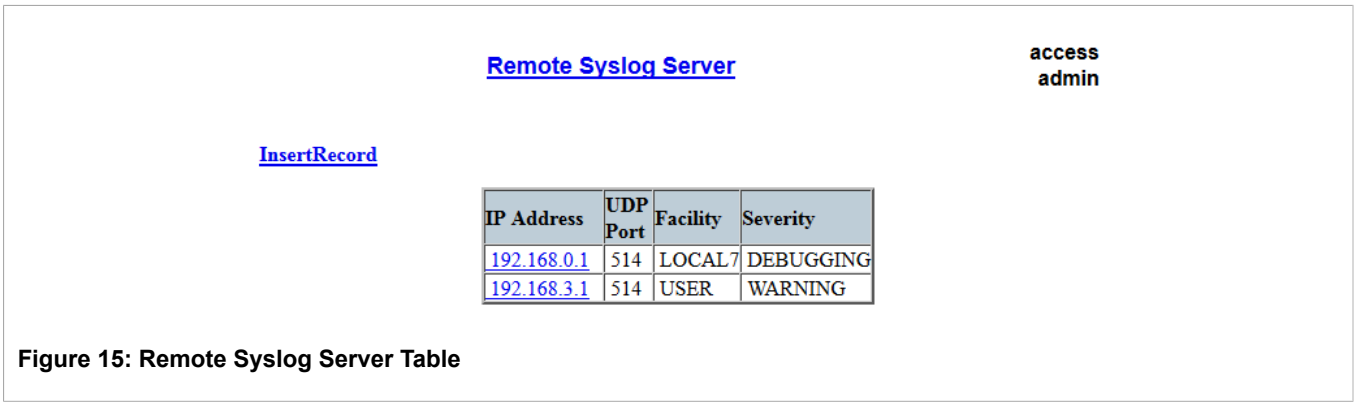


Figure 15: Remote Syslog Server Table

If remote syslog servers have not been configured, add the servers as needed. For more information, refer to Section 3.6.4.3, “Adding a Remote Syslog Server”.

Section 3.6.4.3
Adding a Remote Syslog Server

ROS supports up to 5 remote syslog servers (or collectors). Similar to the local system log, a remote system log server can be configured to log information at a specific severity level. Only messages of a severity level equal to or greater than the specified severity level are written to the log.

To add a remote syslog server to the list of known servers, do the following:

1. Navigate to ***Administration » Configure Syslog » Configure Remote Syslog Server***. The **Remote Syslog Server** table appears.

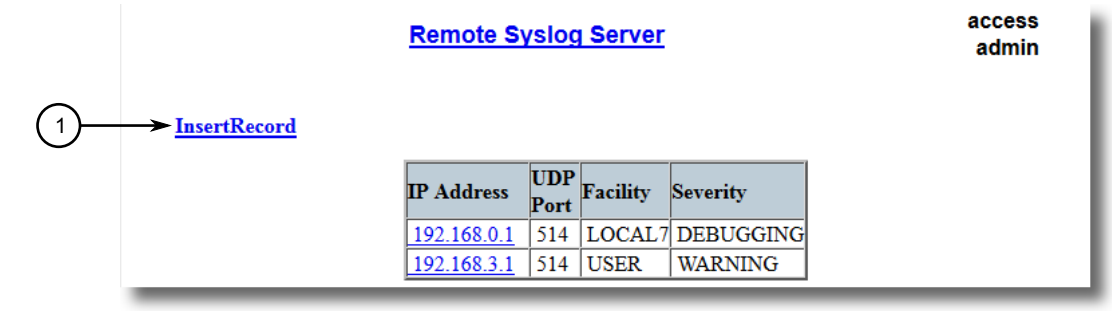


Figure 16: Remote Syslog Server Table

1. InsertRecord

2. Click **InsertRecord**. The **Remote Syslog Server** form appears.

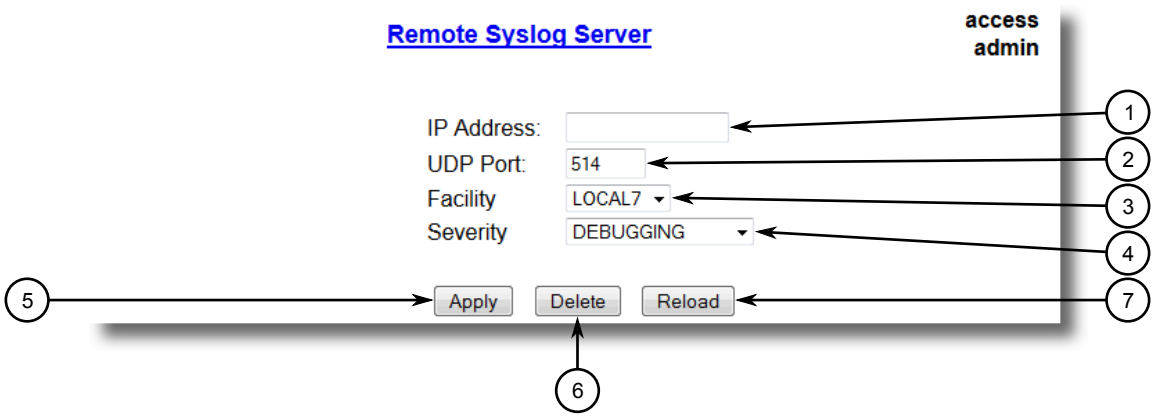


Figure 17: Remote Syslog Server Form

1. IP Address Box **2.** UDP Port Box **3.** Facility Box **4.** Severity Box **5.** Apply Button **6.** Delete Button **7.** Reload Button

3. Configure the following parameter(s) as required:

Parameter	Description
IP Address	**Synopsis:** ###.###.###.### where ### ranges from 0 to 255 Syslog server IP Address.
UDP Port	**Synopsis:** 1025 to 65535 or { 514 } **Default:** 514 The UDP port number on which the remote server listens.
Facility	**Synopsis:** { USER, LOCAL0, LOCAL1, LOCAL2, LOCAL3, LOCAL4, LOCAL5, LOCAL6, LOCAL7 } **Default:** LOCAL7 Syslog Facility is one information field associated with a syslog message. The syslog facility is the application or operating system component that generates a log message. ROS map all syslog logging information onto a single facility which is configurable by user to facilitate remote syslog server.

Parameter	Description
Severity	**Synopsis:** { EMERGENCY, ALERT, CRITICAL, ERROR, WARNING, NOTICE, INFORMATIONAL, DEBUGGING } **Default:** DEBUGGING The severity level is the severity of the message that has been generated. Please note that the severity level user select is accepted as the minimum severity level for the system. For example, if user selects the severity level as 'Error' then the system send any syslog message originated by Error, Critical, Alert and Emergency.

4. Click **Apply**.

Section 3.6.4.4

Deleting a Remote Syslog Server

To delete a remote syslog server from the list of known servers, do the following:

1. Navigate to ***Administration*** » ***Configure Syslog*** » ***Configure Remote Syslog Server***. The **Remote Syslog Server** table appears.

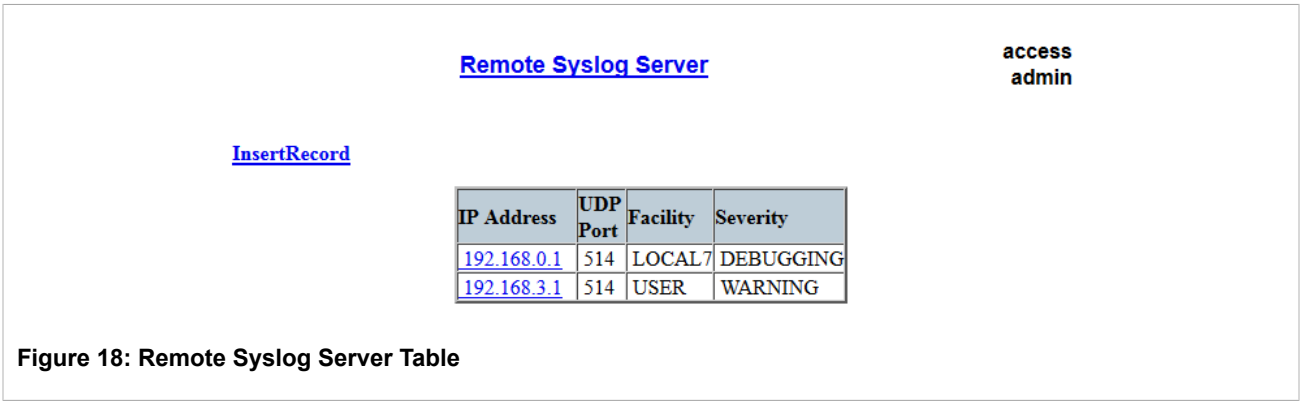


Figure 18: Remote Syslog Server Table

2. Select the server from the table. The **Remote Syslog Server** form appears.

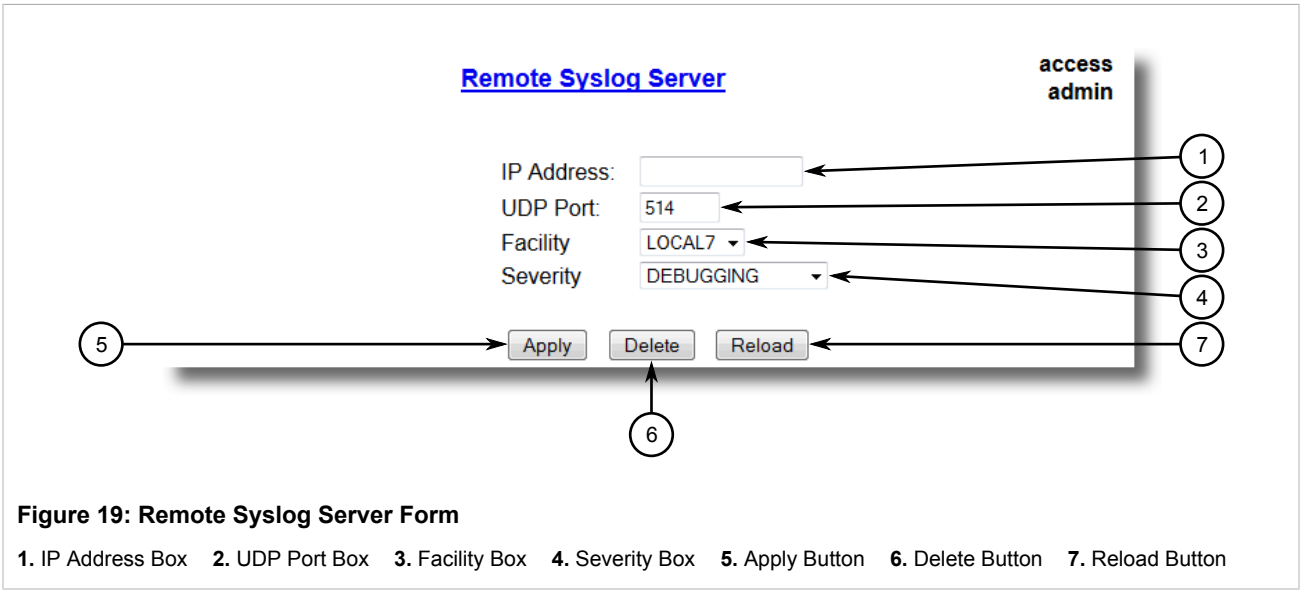


Figure 19: Remote Syslog Server Form

1. IP Address Box **2.** UDP Port Box **3.** Facility Box **4.** Severity Box **5.** Apply Button **6.** Delete Button **7.** Reload Button

3. Click **Delete**.

Section 3.7
Managing IP Gateways

ROS allows up to ten IP gateways to be configured. When both the **Destination** and **Subnet** parameters are blank, the gateway is considered to be a default gateway.

NOTE
The default gateway configuration will not be changed when resetting all configuration parameters to their factory defaults.

The following sections describe how to set up and manage IP gateways:

- Section 3.7.1, “Viewing a List of IP Gateways”
- Section 3.7.2, “Adding an IP Gateway”
- Section 3.7.3, “Deleting an IP Gateway”

Section 3.7.1
Viewing a List of IP Gateways

To view a list of IP gateways configured on the device, navigate to ***Administration » Configure IP Gateways***. The **IP Gateways** table appears.

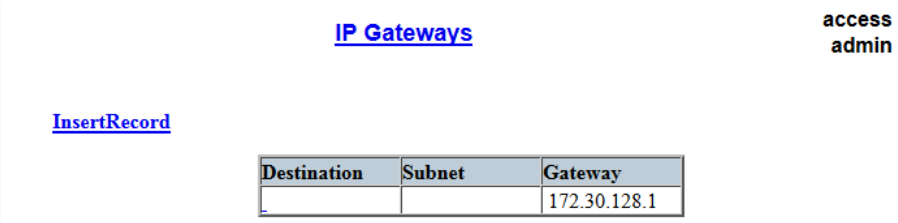


Figure 20: IP Gateways Table

If IP gateways have not been configured, add IP gateways as needed. For more information, refer to Section 3.7.2, “Adding an IP Gateway”.

Section 3.7.2
Adding an IP Gateway

To add an IP gateway, do the following:

1. Navigate to ***Administration » Configure IP Gateways***. The **IP Gateways** table appears.

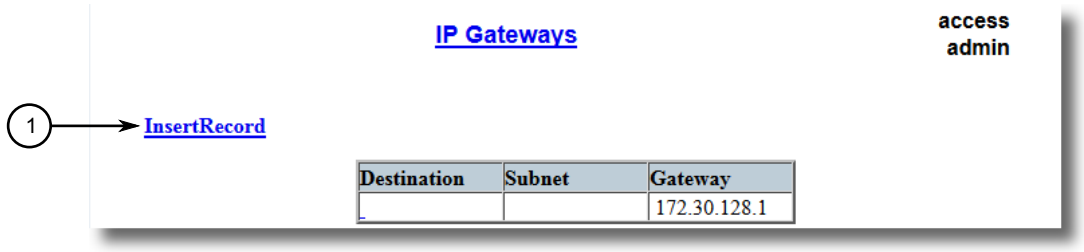


Figure 21: IP Gateways Table

1. InsertRecord

2. Click **InsertRecord**. The **IP Gateways** form appears.

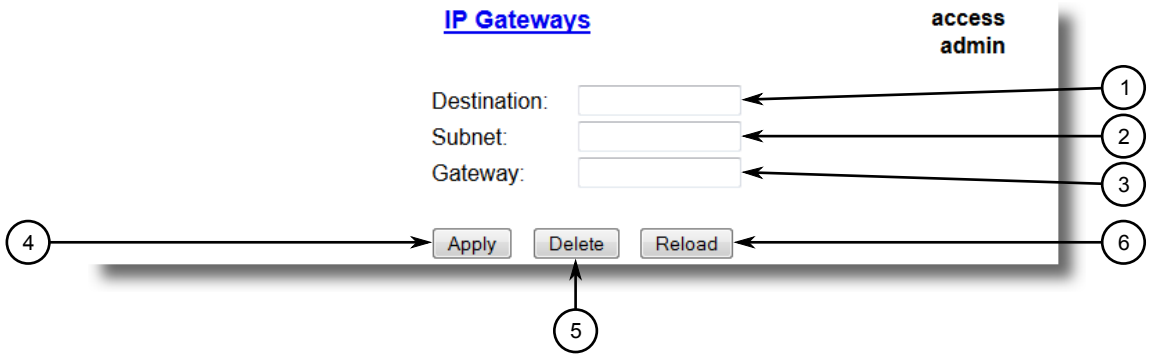


Figure 22: IP Gateways

1. Destination Box **2.** Subnet Box **3.** Gateway Box **4.** Apply Button **5.** Delete Button **6.** Reload Button

3. Configure the following parameter(s) as required:

Parameter	Description
Destination	**Synopsis:** ###.###.###.### where ### ranges from 0 to 255 Specifies the IP address of destination network or host. For default gateway, both the destination and subnet are 0.
Subnet	**Synopsis:** ###.###.###.### where ### ranges from 0 to 255 Specifies the destination IP subnet mask. For default gateway, both the destination and subnet are 0.
Gateway	**Synopsis:** ###.###.###.### where ### ranges from 0 to 255 Specifies the gateway to be used to reach the destination.

4. Click **Apply**.

Section 3.7.3
Deleting an IP Gateway

To delete an IP gateway configured on the device, do the following:

1. Navigate to ***Administration » Configure IP Gateways***. The **IP Gateways** table appears.

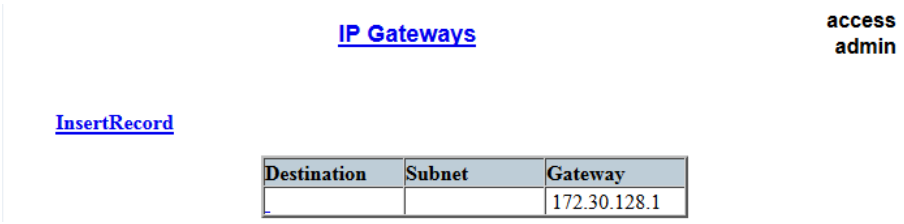


Figure 23: IP Gateways Table

2. Select the IP gateway from the table. The **IP Gateways** form appears.

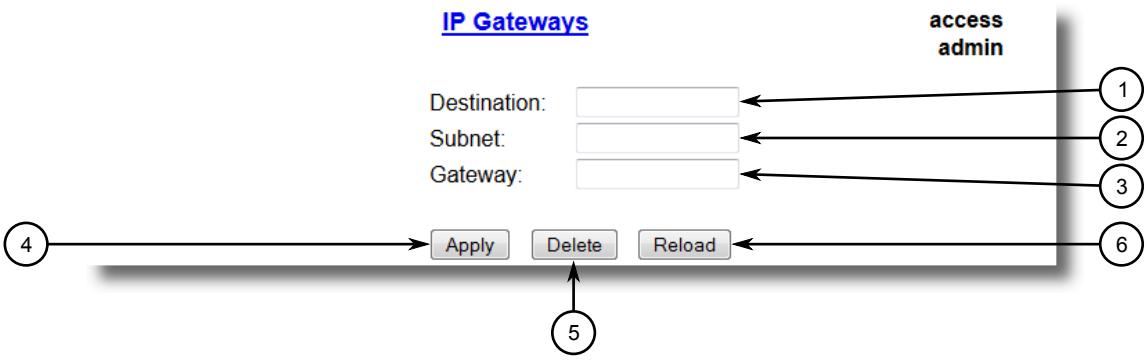


Figure 24: IP Gateways Form

1. Destination Box **2.** Subnet Box **3.** Gateway Box **4.** Apply Button **5.** Delete Button **6.** Reload Button

3. Click **Delete**.

Section 3.8
Configuring IP Services

To configure the IP services provided by the device, do the following:

1. Navigate to ***Administration » Configure IP Services***. The **IP Services** form appears.

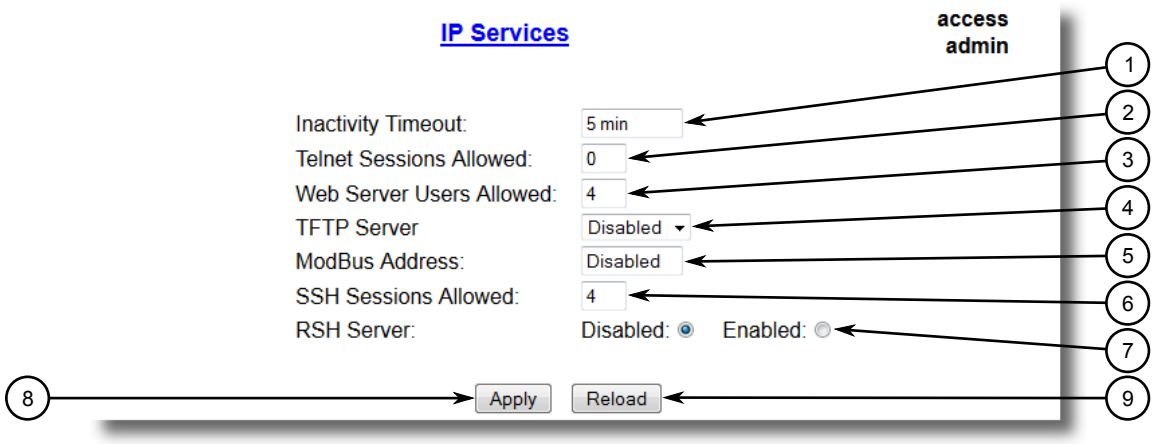


Figure 25: IP Services Form

1. Inactivity Timeout Box **2.** Telnet Sessions Allowed Box **3.** Web Server Users Allowed Box **4.** TFTP Server Box **5.** Modbus Address Box **6.** SSH Sessions Allowed Box **7.** RSH Server Box **8.** Apply Button **9.** Reload Button

2. Configure the following parameter(s) as required:

Parameter	Description
Inactivity Timeout	**Synopsis:** 1 to 60 or { Disabled } **Default:** 5 min Specifies when the console will timeout and display the login screen if there is no user activity. A value of zero disables timeouts. For Web Server users maximum timeout value is limited to 30 minutes.
Telnet Sessions Allowed	**Synopsis:** 0 to 4 **Default:** 0 (controlled version) or 4 (non-controlled version) Limits the number of Telnet sessions. A value of zero prevents any Telnet access.
Web Server Users Allowed	**Synopsis:** 1 to 4 **Default:** 4 Limits the number of simultaneous web server users.
TFTP Server	**Synopsis:** { Disabled, Get Only, Enabled } **Default:** Disabled As TFTP is a very insecure protocol, this parameter allows user to limit or disable TFTP Server access.. DISABLED - disables read and write access to TFTP Server GET ONLY - only allows reading of files via TFTP Server ENABLED - allows reading and writing of files via TFTP Server
ModBus Address	**Synopsis:** 1 to 255 or { Disabled } **Default:** Disabled Determines the Modbus address to be used for Management through Modbus.
SSH Sessions Allowed (Controlled Version Only)	**Synopsis:** 1 to 4 **Default:** 4 Limits the number of SSH sessions.
RSH Server	**Synopsis:** { Disabled, Enabled } **Default:** Disabled (controlled version) or Enabled (non-controlled version)

Parameter	Description
	Disables/enables Remote Shell access.

3. Click **Apply**.

Section 3.9
Managing Remote Monitoring

Remote Monitoring (RMON) is used to collect and view historical statistics related to the performance and operation of Ethernet ports. It can also record a log entry and/or generate an SNMP trap when the rate of occurrence of a specified event is exceeded.

The following sections describe how to configure and manage Remote Monitoring:

- Section 3.9.1, “Managing RMON History Controls”
- Section 3.9.2, “Managing RMON Alarms”
- Section 3.9.3, “Managing RMON Events”

Section 3.9.1
Managing RMON History Controls

The history controls for Remote Monitoring take samples of the RMON-MIB history statistics of an Ethernet port at regular intervals.

The following sections describe how to configure and manage RMON history controls:

- Section 3.9.1.1, “Viewing a List of RMON History Controls”
- Section 3.9.1.2, “Adding an RMON History Control”
- Section 3.9.1.3, “Deleting an RMON History Control”

Section 3.9.1.1
Viewing a List of RMON History Controls

To view a list of RMON history controls, navigate to ***Ethernet Stats » Configure RMON History Controls***. The **RMON History Controls** table appears.

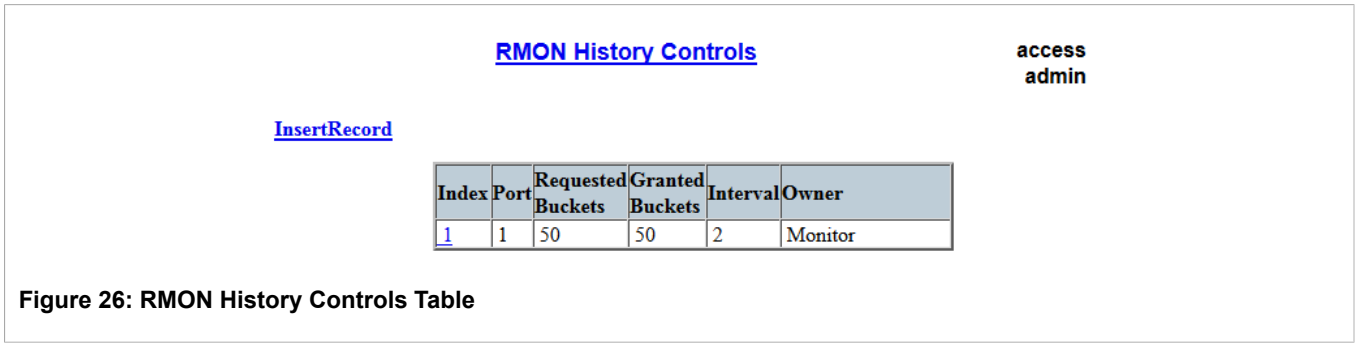


Figure 26: RMON History Controls Table

If history controls have not been configured, add controls as needed. For more information, refer to Section 3.9.1.2, “Adding an RMON History Control”.

Section 3.9.1.2
Adding an RMON History Control

To add an RMON history control, do the following:

1. Navigate to ***Ethernet Stats » Configure RMON History Controls***. The **RMON History Controls** table appears.

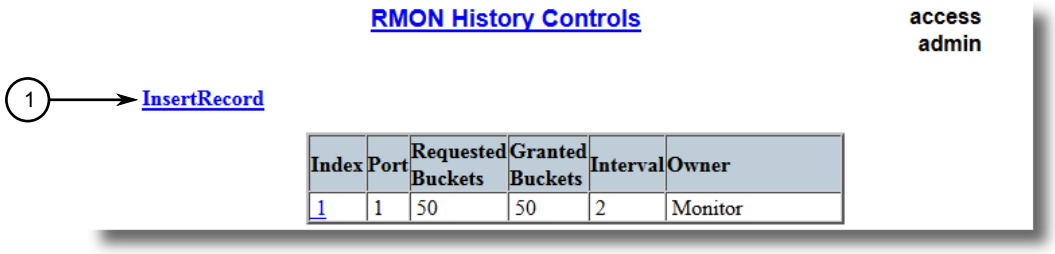


Figure 27: RMON History Controls Table

1. InsertRecord

2. Click **InsertRecord**. The **RMON History Controls** form appears.

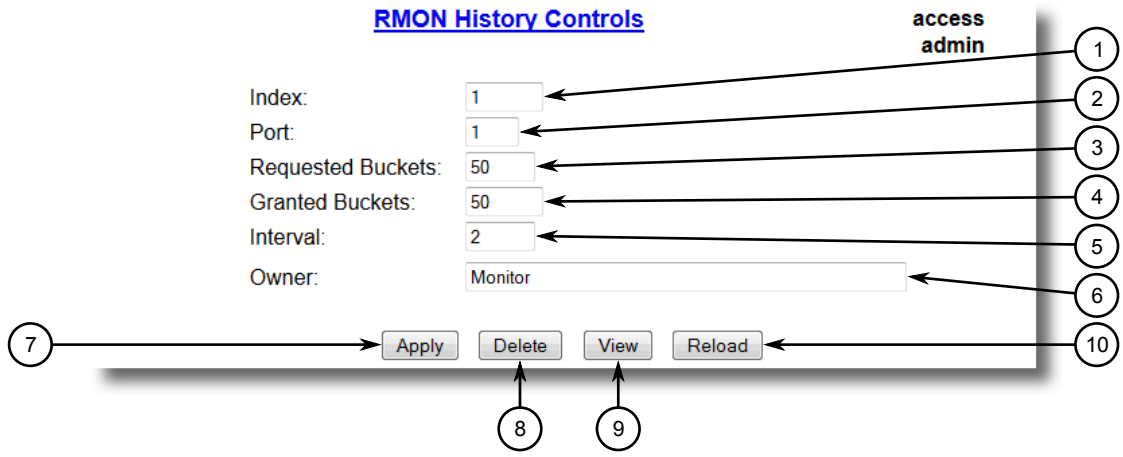


Figure 28: RMON History Controls Form

1. Index Box **2.** Port Box **3.** Requested Buckets Box **4.** Granted Buckets Box **5.** Interval Box **6.** Owner Box **7.** Apply Button **8.** Delete Button **9.** Reload Button

3. Configure the following parameter(s) as required:

Parameter	Description
Index	**Synopsis:** 1 to 65535 **Default:** 1

Parameter	Description
	The index of this RMON History Contol record.
Port	**Synopsis:** 1 to maximum port number **Default:** 1 The port number as seen on the front plate silkscreen of the switch.
Requested Buckets	**Synopsis:** 1 to 4000 **Default:** 50 The maximum number of buckets requested for this RMON collection history group of statistics. The range is 1 to 4000. The default is 50.
Granted Buckets	**Synopsis:** 0 to 65535 The number of buckets granted for this RMON collection history. This field is not editable.
Interval	**Synopsis:** 1 to 3600 **Default:** 1800 The number of seconds in over which the data is sampled for each bucket. The range is 1 to 3600. The default is 1800.
Owner	**Synopsis:** Any 127 characters **Default:** Monitor The owner of this record. It is suggested to start this string withword 'monitor'.

4. Click **Apply**.

Section 3.9.1.3
Deleting an RMON History Control

To delete an RMON history control, do the following:

1. Navigate to ***Ethernet Stats*** » ***Configure RMON History Controls***. The **RMON History Controls** table appears.

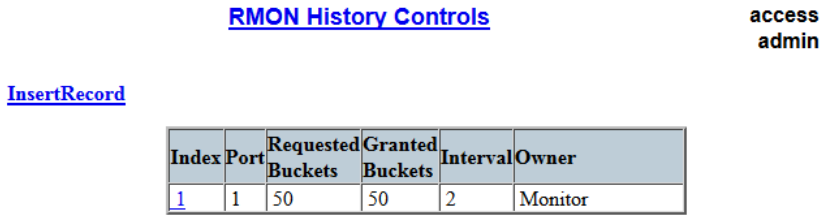


Figure 29: RMON History Controls Table

2. Select the history control from the table. The **RMON History Controls** form appears.

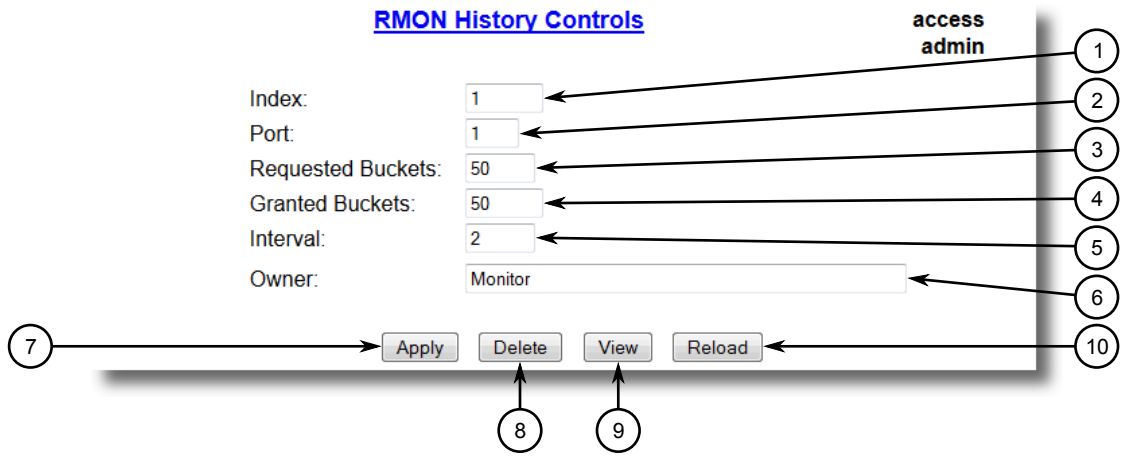


Figure 30: RMON History Controls Form

1. Index Box **2.** Port Box **3.** Requested Buckets Box **4.** Granted Buckets Box **5.** Interval Box **6.** Owner Box **7.** Apply Button **8.** Delete Button **9.** Reload Button

3. Click **Delete**.

Section 3.9.2

Managing RMON Alarms

When Remote Monitoring (RMON) alarms are configured, ROS examines the state of a specific statistical variable.

Remote Monitoring (RMON) alarms define upper and lower thresholds for legal values of specific statistical variables in a given interval. This allows ROS to detect events as they occur more quickly than a specified maximum rate or less quckly than a minimum rate.

When the rate of change for a statistics value exceeds its limits, an internal INFO alarm is always generated. For information about viewing alarms, refer to Section 4.4.2, “Viewing and Clearing Latched Alarms”.

Additionally, a statistic threshold crossing can result in further activity. An RMON alarm can be configured to point to a particular RMON event, which can generate an SNMP trap, an entry in the event log, or both. The RMON event can also direct alarms towards different users defined for SNMP.

The alarm can point to a different event for each of the thresholds. Therefore, combinations such as *trap on rising threshold* or *trap on rising threshold, log and trap on falling threshold* are possible.

Each RMON alarm may be configured such that its first instance occurs only for rising, falling, or all thresholds that exceed their limits.

The ability to configure upper and lower thresholds on the value of a measured statistic provides for the ability to add hysteresis to the alarm generation process.

If the value of the measured statistic over time is compared to a single threshold, alarms will be generated each time the statistic crosses the threshold. If the statistic’s value fluctuates around the threshold, an alarm can be generated every measurement period. Programming different upper and lower thresholds eliminates spurious alarms. The statistic value must *travel* between the thresholds before alarms can be generated. The following illustrates the very different patterns of alarm generation resulting from a statistic sample and the same sample with hysteresis applied.

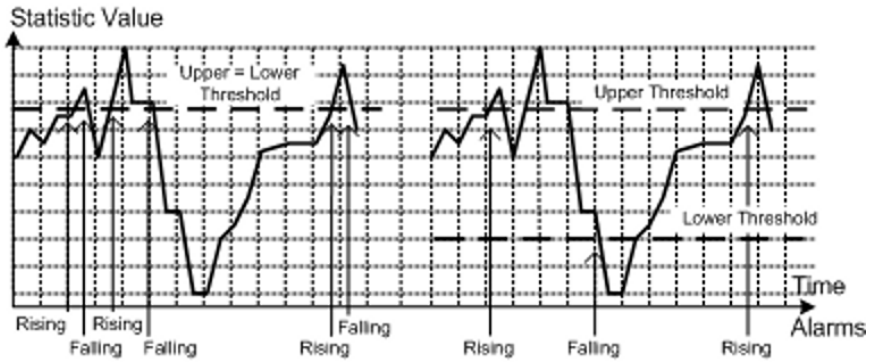


Figure 31: The Alarm Process

There are two methods to evaluate a statistic in order to determine when to generate an event: delta and absolute.

For most statistics, such as line errors, it is appropriate to generate an alarm when a rate is exceeded. The alarm defaults to the *delta* measurement method, which examines changes in a statistic at the end of each measurement period.

It may be desirable to alarm when the total, or absolute, number of events crosses a threshold. In this case, set the measurement period type to *absolute*.

The following sections describe how to configure and manage RMON alarms:

- Section 3.9.2.1, “Viewing a List of RMON Alarms”
- Section 3.9.2.2, “Adding an RMON Alarm”
- Section 3.9.2.3, “Deleting an RMON Alarm”

Section 3.9.2.1
Viewing a List of RMON Alarms

To view a list of RMON alarms, navigate to ***Ethernet Stats » Configure RMON Alarms***. The **RMON Alarms** table appears.

RMON Alarms

access
admin

InsertRecord

Index	Variable	Rising Thr	Falling Thr	Value	Type	Interval	Star
1	ifInOctets.1	150	100	0	delta	1	risin

Figure 32: RMON Alarms Table

If alarms have not been configured, add alarms as needed. For more information, refer to Section 3.9.2.2, “Adding an RMON Alarm”.

Section 3.9.2.2
Adding an RMON Alarm

To add an RMON alarm, do the following:

1. Navigate to ***Ethernet Stats*** » ***Configure RMON Alarms***. The **RMON Alarms** table appears.

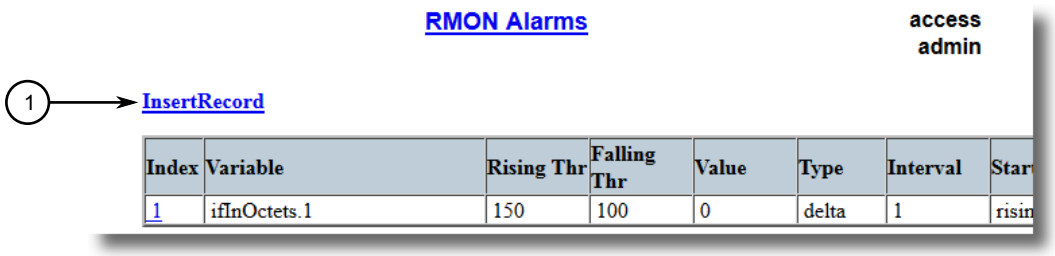


Figure 33: RMON Alarms Table

1. InsertRecord

2. Click **InsertRecord**. The **RMON Alarms** form appears.

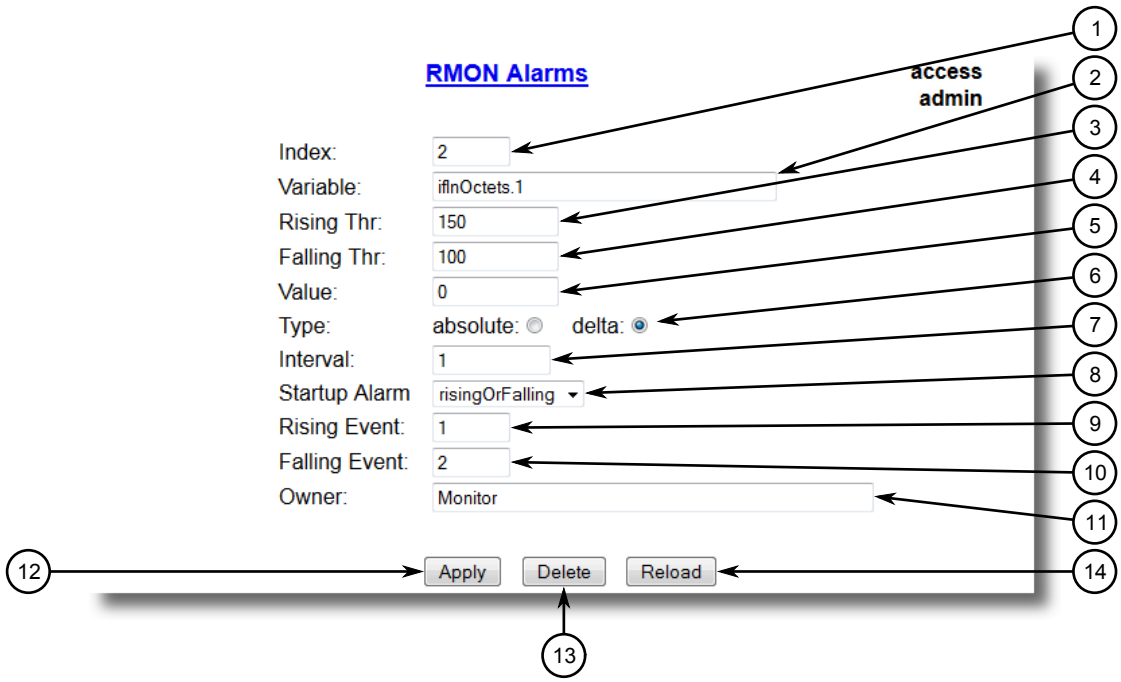


Figure 34: RMON Alarms Form

1. Index Box **2.** Variable Box **3.** Rising Thr Box **4.** Falling Thr Box **5.** Value Box **6.** Type Options **7.** Interval Box **8.** Startup Alarm List **9.** Rising Event Box **10.** Falling Event Box **11.** Owner Box **12.** Apply Button **13.** Delete Button **14.** Reload Button

3. Configure the following parameter(s) as required:

Parameter	Description
Index	**Synopsis:** 1 to 65535 **Default:** 1 The index of this RMON Alarm record.
Variable	**Synopsis:** SNMP Object Identifier - up to 39 characters The SNMP object identifier (OID) of the particular variable to be sampled. Only variables that resolve to an ASN.1 primitive type INTEGER (INTEGER, Integer32,Counter32, Counter64, Gauge, or TimeTicks) may be sampled. A list of objects can be printed using shell command 'rmon'. The OID format: objectName.index1.index2... where index format depends on index object type.
Rising Thr	**Synopsis:** -2147483647 to 2147483647 **Default:** 0 A threshold for the sampled variable. When the current sampled variable value is greater than or equal to this threshold, and the value at the last sampling interval was less than this threshold, a single event will be generated. A single event will also be generated if the first sample after this record is created is greater than or equal to this threshold and the associated startup alarm ils equal to 'rising'.After rising alarm is generated, another such event will not be generated until the sampled value falls below this threshold and reaches the value of FallingThreshold.
Falling Thr	**Synopsis:** -2147483647 to 2147483647 **Default:** 0 A threshold for the sampled variable. When the current sampled variable value is less than or equal to this threshold, and the value at the last sampling interval was greater than this threshold, a single event will be generated. A single event will also be generated if the first sample after this record is created is less than or equal to this threshold and the associated startup alarm ils equal to 'falling'.After falling alarm is generated, another such event will not be generated until the sampled value rises above this threshold and reaches the value of RisingThreshold.
Value	**Synopsis:** -2147483647 to 2147483647 The value of monitoring object during the last sampling period. The presentation of value depends of sample type ('absolute' or 'delta').
Type	**Synopsis:** { absolute, delta } **Default:** delta The method of sampling the selected variable and calculating the value to be compared against the thresholds. The value of sample type can be 'absolute' or 'delta'.
Interval	**Synopsis:** 0 to 2147483647 **Default:** 60 The number of seconds in over which the data is sampled and compared with the rising and falling thresholds.
Startup Alarm	**Synopsis:** { rising, falling, risingOrFalling } **Default:** risingOrFalling The alarm that may be sent when this record is first created if condition for raising alarm is met. The value of startup alarm can be 'rising', 'falling' or 'risingOrFalling'.
Rising Event	**Synopsis:** 0 to 65535 **Default:** 0 The index of the event that is used when a falling threshold is crossed. If there is no corresponding entryl in the Event Table, then no association exists. In particular, if this value is zero, no associated event will be generated.
Falling Event	**Synopsis:** 0 to 65535 **Default:** 0

Parameter	Description
	The index of the event that is used when a rising threshold is crossed. If there is no corresponding entryl in the Event Table, then no association exists. In particular, if this value is zero, no associated event will be generated.
Owner	**Synopsis:** Any 127 characters **Default:** Monitor The owner of this record. It is suggested to start this string withword 'monitor'.

4. Click **Apply**.

Section 3.9.2.3
Deleting an RMON Alarm

To delete an RMON alarm, do the following:

1. Navigate to ***Ethernet Stats » Configure RMON Alarms***. The **RMON Alarms** table appears.

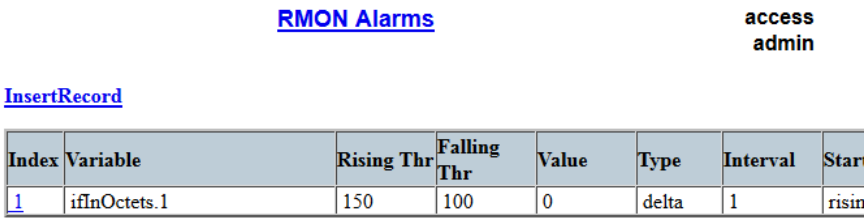


Figure 35: RMON Alarms Table

2. Select the alarm from the table. The **RMON Alarms** form appears.

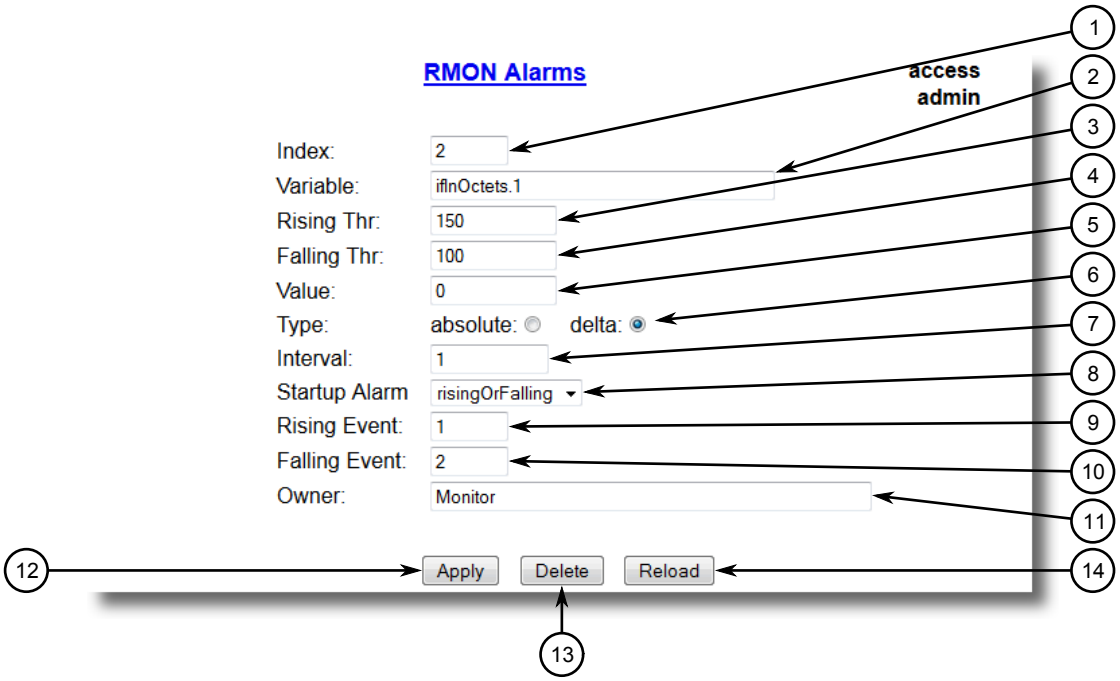


Figure 36: RMON Alarms Form

1. Index Box **2.** Variable Box **3.** Rising Thr Box **4.** Falling Thr Box **5.** Value Box **6.** Type Options **7.** Interval Box **8.** Startup Alarm List **9.** Rising Event Box **10.** Falling Event Box **11.** Owner Box **12.** Apply Button **13.** Delete Button **14.** Reload Button

3. Click **Delete**.

Section 3.9.3

Managing RMON Events

Remote Monitoring (RMON) events define behavior profiles used in event logging. These profiles are used by RMON alarms to send traps and log events.

Each alarm may specify that a log entry be created on its behalf whenever the event occurs. Each entry may also specify that a notification should occur by way of SNMP trap messages. In this case, the user for the trap message is specified as the *Community*.

Two traps are defined: risingAlarm and fallingAlarm.

The following sections describe how to configure and manage RMON events:

- Section 3.9.3.1, “Viewing a List of RMON Events”
- Section 3.9.3.2, “Adding an RMON Event”
- Section 3.9.3.3, “Deleting an RMON Event”

Section 3.9.3.1
Viewing a List of RMON Events

To view a list of RMON events, navigate to ***Ethernet Stats*** » ***Configure RMON Events***. The **RMON Events** table appears.

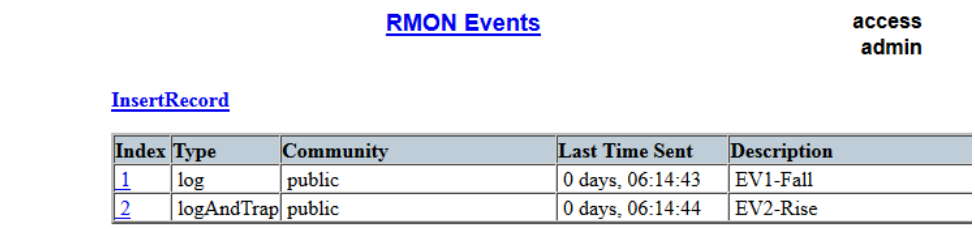


Figure 37: RMON Events Table

If events have not been configured, add events as needed. For more information, refer to Section 3.9.3.2, “Adding an RMON Event”.

Section 3.9.3.2
Adding an RMON Event

To add an RMON alarm, do the following:

1. Navigate to ***Ethernet Stats*** » ***Configure RMON Events***. The **RMON Events** table appears.

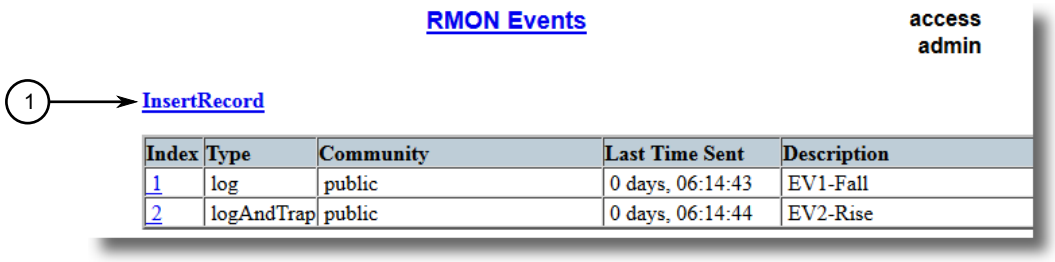


Figure 38: RMON Events Table

1. InsertRecord

2. Click **InsertRecord**. The **RMON Events** form appears.

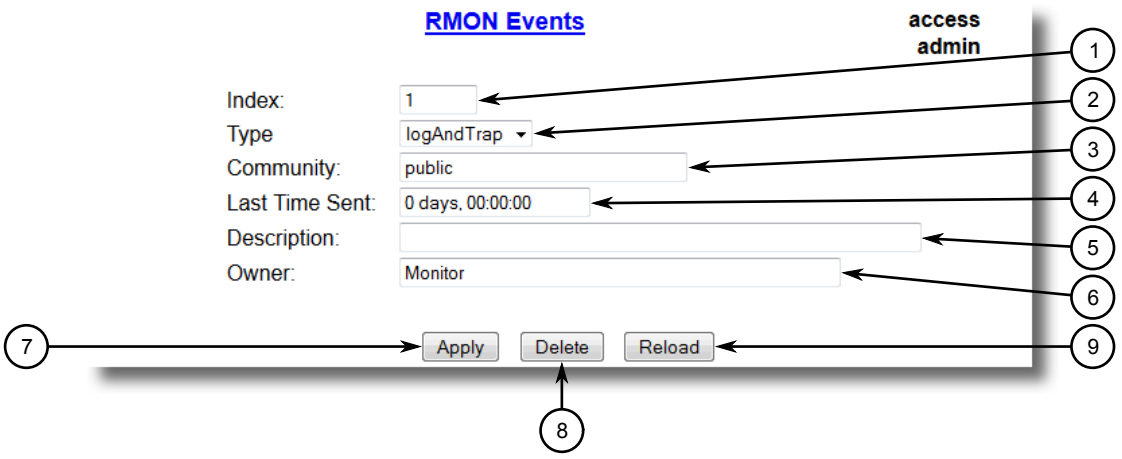


Figure 39: RMON Events Form

1. Index Box **2.** Type List **3.** Community Box **4.** Last Time Sent Box **5.** Description Box **6.** Owner Box **7.** Apply Button **8.** Delete Button **9.** View Button **10.** Reload Button

3. Configure the following parameter(s) as required:

Parameter	Description
Index	**Synopsis:** 1 to 65535 **Default:** 3 The index of this RMON Event record.
Type	**Synopsis:** { none, log, snmpTrap, logAndTrap } **Default:** logAndTrap The type of notification that the probe will make about this event. In the case of 'log', an entry is made in the RMON Log table for each event. In the case of snmp_trap, an SNMP trap is sent to one or more management stations.
Community	**Synopsis:** Any 31 characters **Default:** public If the SNMP trap is to be sent, it will be sent to the SNMP community specified by this string.
Last Time Sent	**Synopsis:** DDDD days, HH:MM:SS The time from last reboot at the time this event entry last generated an event. If this entry has not generated any events, this value will be 0.
Description	**Synopsis:** Any 127 characters **Default:** EV2-Rise A comment describing this event.
Owner	**Synopsis:** Any 127 characters **Default:** Monitor The owner of this event record. It is suggested to start this string withword 'monitor'.

4. Click **Apply**.

Section 3.9.3.3
Deleting an RMON Event

To delete an RMON event, do the following:

1. Navigate to ***Ethernet Stats*** » ***Configure RMON Events***. The **RMON Events** table appears.

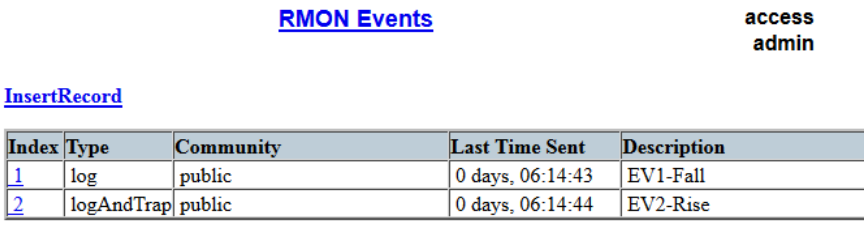


Figure 40: RMON Events Table

2. Select the event from the table. The **RMON Events** form appears.

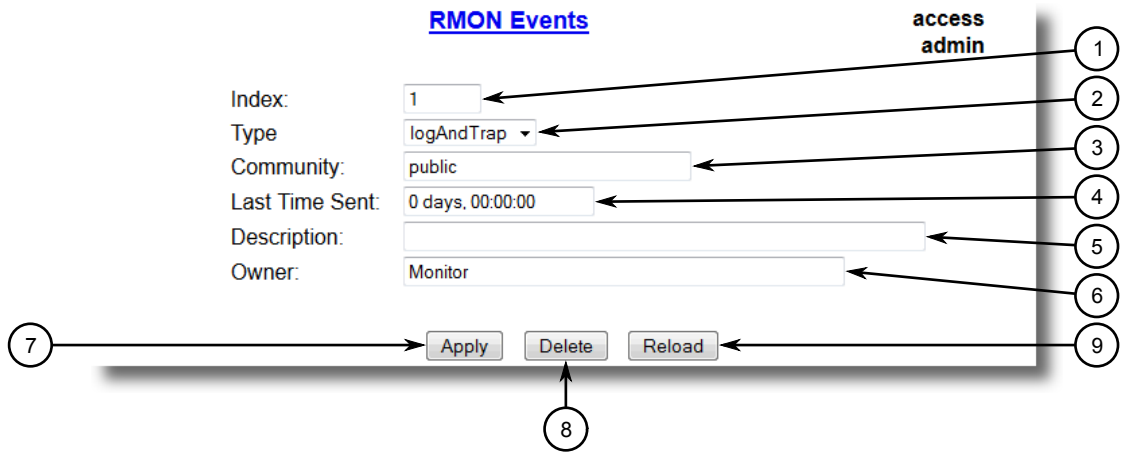


Figure 41: RMON Events Form

1. Index Box **2.** Type List **3.** Community Box **4.** Last Time Sent Box **5.** Description Box **6.** Owner Box **7.** Apply Button **8.** Delete Button **9.** View Button **10.** Reload Button

3. Click **Delete**.

Section 3.10
Upgrading/Downgrading Firmware

The following sections describe how to upgrade and downgrade the firmware:

- Section 3.10.1, “Upgrading Firmware”
- Section 3.10.2, “Downgrading Firmware”

Section 3.10.1
Upgrading Firmware

Upgrading ROS firmware, including the main, bootloader and FPGA firmware, may be necessary to take advantage of new features or bug fixes. Binary firmware images are available from Siemens . Visit www.siemens.com/ruggedcom to determine which versions/updates are available or contact Siemens Customer Support.

Binary firmware images transferred to the device are stored in non-volatile Flash memory and require a device reset in order to take effect.

IMPORTANT!
Non-Controlled (NC) versions of ROS can not be upgraded to Controlled firmware versions. However, Controlled firmware versions can be upgraded to an NC firmware version.

NOTE
The IP address set for the device will not be changed following a firmware upgrade.

To upgrade the ROS firmware, do the following:

1.
2. Reset the device to complete the installation. For more information, refer to Section 3.11, “Resetting the Device”.
3. Access the CLI shell and verify the new software version has been installed by typing **`version`**. The currently installed versions of the main and boot firmware are displayed.

Section 3.10.2
Downgrading Firmware

Downgrading the ROS firmware is generally not recommended, as it may have unpredictable effects. However, if a downgrade is required, do the following:

IMPORTANT!
Before downgrading the firmware, make sure the hardware and FPGA code types installed in the device are supported by the older firmware version. Refer to the Release Notes for the older firmware version to confirm.

IMPORTANT!
Non-Controlled (NC) versions of ROS can not be downgraded to Controlled firmware versions. However, Controlled firmware versions can be downgraded to an NC firmware version.

CAUTION!
Do not downgrade the ROS boot version.

1. Disconnect the device from the network.
2. Log in to the device as an admin user. For more information, refer to Section 2.2, “Logging In”.
3. Make a local copy of the current configuration file. For more information, refer to Section 3.5, “Uploading/ Downloading Files”.

IMPORTANT!
Never downgrade the ROS software version beyond ROS v4.1 when encryption is enabled. Make sure the device has been restored to factory defaults before downgrading.

4. Restore the device to its factory defaults. For more information, refer to Section 3.3, “Restoring Factory Defaults”.
5. Upload and apply the older firmware version and its associated FPGA files using the same methods used to install newer firmware versions. For more information , refer to Section 3.10.1, “Upgrading Firmware”.
6. Press **Ctrl-S** to access the CLI.
7. Clear all logs by typing:

```
clearlogs
```

8. Clear all alarms by typing:

```
clearalarms
```

IMPORTANT!
After downgrading the firmware and FPGA files, be aware that some settings from the previous configuration may be lost or reverted back to the factory defaults (including user’s passwords if downgrading from a security related version), as those particular tables or fields may not exist in the older firmware version. Because of this, the unit must be configured after the downgrade.

9. Configure the device as required.

Section 3.11
Resetting the Device

To reset the device, do the following:

1. Navigate to ***Diagnostics*** » ***Reset Device***. The **Reset Device** form appears.

Figure 42: Reset Device Form

1. Confirm Button

2. Click **Confirm**.

Section 3.12

Decommissioning the Device

Before taking the device out of service, either permanently or for maintenance by a third-party, make sure the device has been fully decommissioned. This includes removing any sensitive, proprietary information.

To decommission the device, do the following:

1. Disconnect all network cables from the device.
2. Connect to the device via the RS232 serial console port. For more information, refer to Section 2.1.1, "Connecting Directly".
3. Restore all factory default settings for the device. For more information, refer to Section 3.3, "Restoring Factory Defaults".
4. Access the CLI. For more information, refer to Section 2.6, "Using the Command Line Interface".
5. Upload a blank version of the `banner.txt` file to the device to replace the existing file. For more information about uploading a file, refer to Section 3.5, "Uploading/Downloading Files".
6. Confirm the upload was successful by typing:

   ```
   type banner.txt
   ```

7. Clear the system and crash logs by typing:

   ```
   clearlog
   ```

8. Generate a random SSL certificate by typing:

   ```
   sslkeygen
   ```

   This may take several minutes to complete. To verify the certificate has been generated, type:

   ```
   type syslog.txt
   ```

   When the phrase

   ```
   Generated ssl.crt was saved
   ```

   appears in the log, the SSL certificate has been generated.
9. Generate random SSH keys by typing:

   ```
   sshkeygen
   ```

   This may take several minutes to complete. To verify the keys have been generated, type:

   ```
   type syslog.txt
   ```

   When the phrase

   ```
   Generated ssh.keys was saved
   ```

   appears in the log, the SSH keys have been generated.
10. De-fragment and erase all free flash memory by typing:

    ```
    flashfile defrag
    ```

    This may take several minutes to complete.

4 System Administration

This chapter describes how to perform various administrative tasks related to device identification, user permissions, alarm configuration, certificates and keys, and more. It describes the following tasks:

- Section 4.1, “Configuring the System Information”
- Section 4.2, “Customizing the Login Screen”
- Section 4.3, “Configuring Passwords”
- Section 4.4, “Managing Alarms”
- Section 4.5, “Managing the Configuration File”
- Section 4.6, “Managing an Authentication Server”

Section 4.1

Configuring the System Information

To configure basic information that can be used to identify the device, its location, and/or its owner, do the following:

1. Navigate to ***Administration » Configure System Identification***. The **System Identification** form appears.

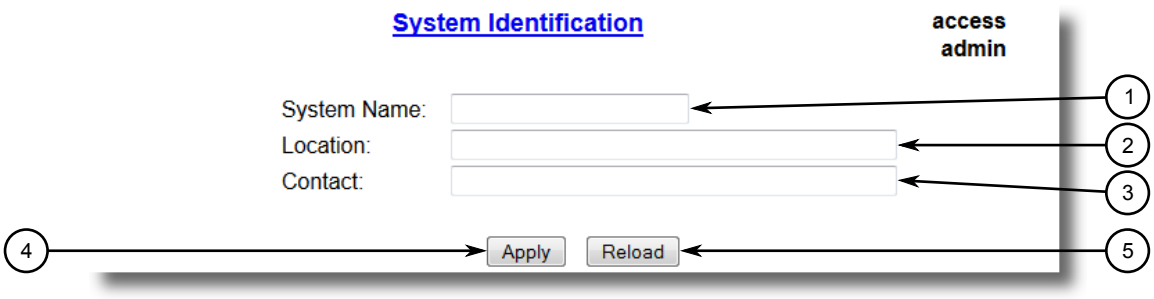


Figure 43: System Identification Form

1. System Name Box **2.** Location Box **3.** Contact Box **4.** Apply Button **5.** Reload Button

2. Configure the following parameter(s) as required:

Parameter	Description
System Name	**Synopsis:** Any 24 characters The system name is displayed in all ROS menu screens. This can make it easier to identify the switches within your network provided that all switches are given a unique name.
Location	**Synopsis:** Any 49 characters The location can be used to indicate the physical location of the switch. It is displayed in the login screen as another means to ensure you are dealing with the desired switch.

Parameter	Description
Contact	**Synopsis:** Any 49 characters The contact can be used to help identify the person responsible for managing the switch. You can enter name, phone number, email, etc. It is displayed in the login screen so that this person may be contacted should help be required.

3. Click **Apply**.

Section 4.2
Customizing the Login Screen

To display a custom welcome message, device information or any other information on the login screen for the Web and console interfaces, add text to the `banner.txt` file stored on the device. If the `banner.txt` file is empty, only the **Username** and **Password** fields appear on the login screen.

To update the `banner.txt` file, download the file from the device, modify it and then load it back on to the device. For information about uploading and downloading files, refer to Section 3.5, “Uploading/Downloading Files”.

Section 4.3
Configuring Passwords

ROS allows for up to three user profiles to be configured locally on the device. Each profile corresponds to one of the following access levels:

- Guest
- Operator
- Admin

The access levels provide or restrict the user's ability to change settings and execute various commands.

Rights	User Type		
	Guest	Operator	Admin
View Settings	✓	✓	✓
Clear Logs	×	✓	✓
Reset Alarms	×	✓	✓
Clear Statistics	×	✓	✓
Change Basic Settings	×	✓	✓
Change Advanced Settings	×	×	✓
Run Commands	×	×	✓

Default passwords are configured for each user type initially. It is strongly recommended that these be changed before the device is commissioned.

NOTE
Users can also be verified through a RADIUS or TACACS+ server. When enabled for authentication and authorization, the RADIUS or TACACS+ server will be used in the absence of any local settings. For more information about configuring a RADIUS or TACACS+ server, refer to Section 4.6, "Managing an Authentication Server".

CAUTION!
To prevent unauthorized access to the device, make sure to change the default passwords for each profile before commissioning the device.

To configure passwords for one or more of the user profiles, do the following:

1. Navigate to ***Administration*** » ***Configure Passwords***. The **Configure Passwords** form appears.

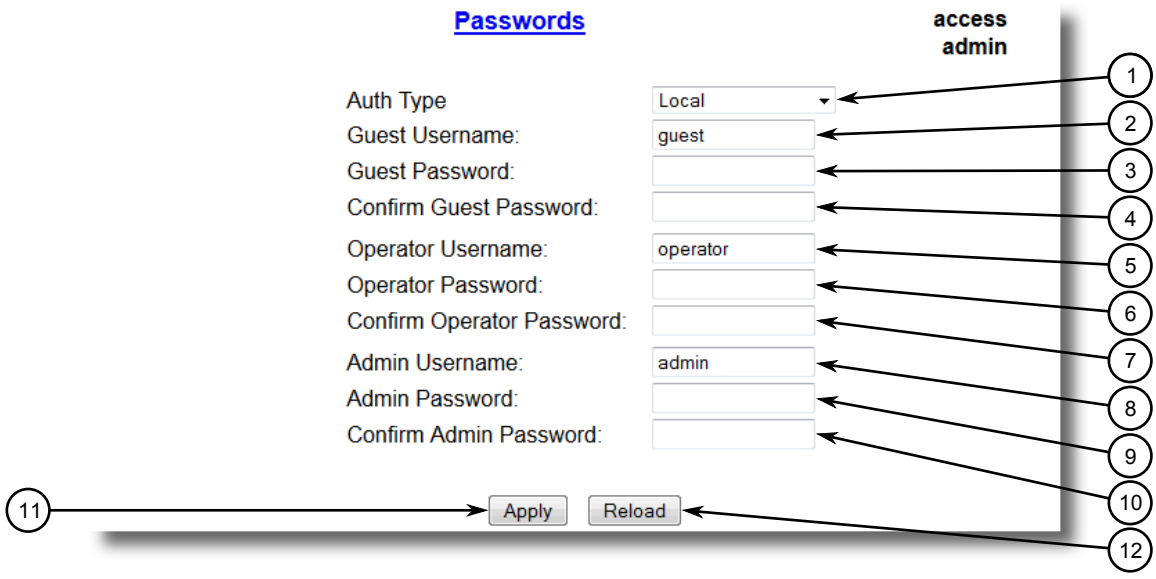


Figure 44: Configure Passwords Form

1. Auth Type Box **2.** Guest Username Box **3.** Guest Password Box **4.** Confirm Guest Password Box **5.** Operator Username Box **6.** Operator Password Box **7.** Confirm Operator Password Box **8.** Admin Username Box **9.** Admin Password Box **10.** Confirm Admin Password Box **11.** Apply Button **12.** Reload Button

NOTE
ROS requires that all user passwords meet strict guidelines to prevent the use of weak passwords. When creating a new password, make sure it adheres to the following rules:

- *Must not be less than 8 characters in length.*
- *Must not include the username or any 4 continous characters found in the username. For example, if the username is Subnet25, the password may not be subnet25admin, subnetadmin or net25admin. However, net-25admin or Sub25admin is permitted.*
- *Must have at least one alphabetic character and one number. Special characters are permitted.*
- *Must not have more than 3 continuously incrementing or decrementing numbers. For example, Sub123 and Sub19826 are permitted, but Sub12345 is not.*

An alarm will generate if a weak password is configured. The weak password alarm can be disabled by the user. For more information about disabling alarms, refer to Section 4.4, "Managing Alarms".

2. Configure the following parameter(s) as required:

Parameter	Description
Auth Type	**Synopsis:** { Local, RADIUS, TACACS+, RADIUSorLocal, TACACS+orLocal } **Default:** Local Password can be authenticated using localy configured values, or remote RADIUS or TACACS+ server. Setting value to any of combinations that involve RADIUS or TACACS + require Security Server Table to be configured. Settings: • Local - Authentication from the local Password Table. • RADIUS - Authentication using a RADIUS server. • TACACS+ - Authentication using a TACACS+ server. • RADIUSOrLocal - Authentication using RADIUS. If the server cannot be reached, authenticate from the local Password Table. • TACACS+OrLocal - Authentication using TACACS+. If the server cannot be reached, authenticate from the local Password Table **NOTE** *For console access, local credentials will always be checked first regardless of the device configuration. If server authentication is required, requests to the server will be sent only if local authentication fails.*
Guest Username	**Synopsis:** Any 15 characters **Default:** guest Related password is in field Guest Password; view only, cannot change settings or run any commands.
Guest Password	**Synopsis:** 15 character ASCII string Related username is in field Guest Username; view only, cannot change settings or run any commands.
Confirm Guest Password	**Synopsis:** 15 character ASCII string Related username is in field Guest Username; view only, cannot change settings or run any commands.
Operator Username	**Synopsis:** Any 15 characters **Default:** operator Related password is in field Oper Password; cannot change settings; can reset alarms, statistics, logs, etc.
Operator Password	**Synopsis:** 15 character ASCII string Related username is in field Oper Username; cannot change settings; can reset alarms, statistics, logs, etc
Confirm Operator Password	**Synopsis:** 15 character ASCII string Related username is in field Oper Username; cannot change settings; can reset alarms, statistics, logs, etc.
Admin Username	**Synopsis:** Any 15 characters **Default:** admin Related password is in field Admin Password; full read/write access to all settings and commands.
Admin Password	**Synopsis:** 15 character ASCII string

Parameter	Description
	Related username is in field Admin Username; full read/write access to all settings and commands.
Confirm Admin Password	**Synopsis:** 15 character ASCII string Related username is in field Admin Username; full read/write access to all settings and commands.

3. Click **Apply**.

Section 4.4

Managing Alarms

Alarms indicate the occurrence of events of either importance or interest that are logged by the device.

There are two types of alarms:

- **Active alarms** signify states of operation that are not in accordance with normal operation. Examples include links that should be up, but are not, or error rates that repeatedly exceed a certain threshold. These alarms are continuously active and are only cleared when the problem that triggered the alarms is resolved.
- **Passive alarms** are a record of abnormal conditions that occurred in the past and do not affect th current operation state of the device. Examples include authentication failures, Remote Network MONitoring (RMON) MIB generated alarms, or error states that temporarily exceeded a certain threshold . These alarms can be cleared from the list of alarms.

NOTE
For more information about RMON alarms, refer to Section 3.9.2, "Managing RMON Alarms".

When either type of alarm occurs, a message appears in the top right corner of the user interface. If more than one alarm has occurred, the message will indicate the number of alarms. Active alarms also trip the Critical Failure Relay LED on the device. The message and the LED will remain active until the alarm is cleared.

NOTE
Alarms are volatile in nature. All alarms (active and passive) are cleared at startup.

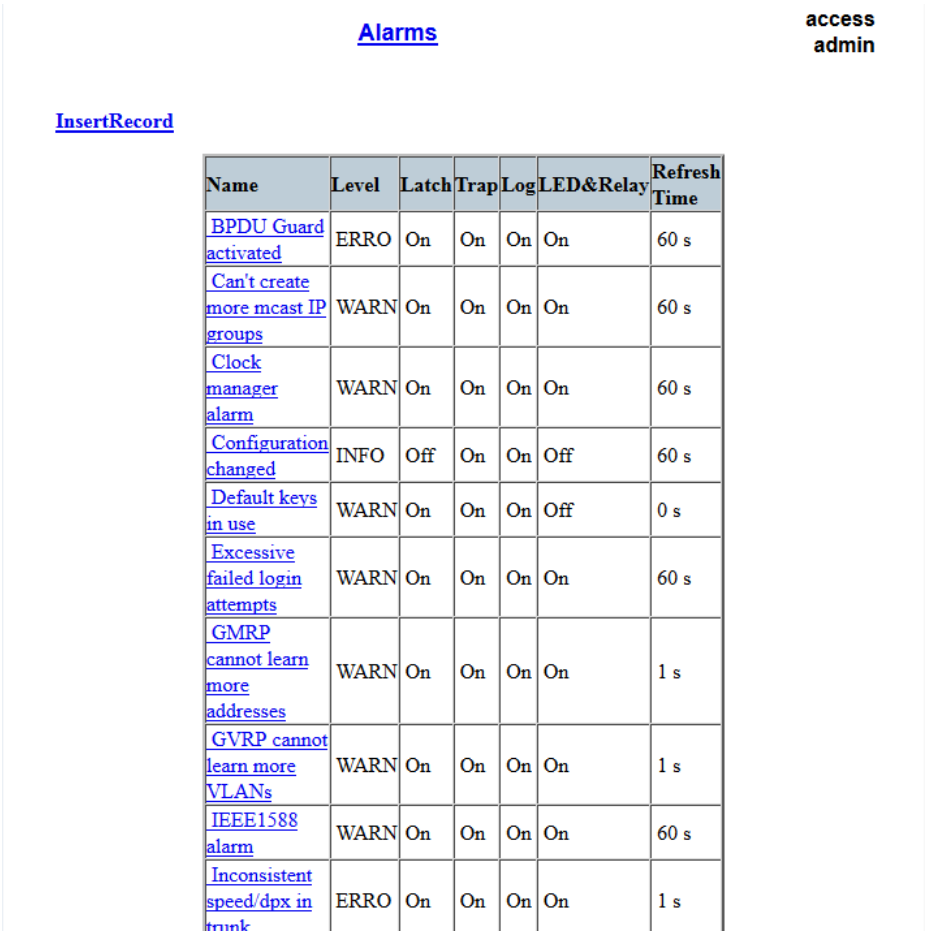
The following sections describe how to set up and manage alarms:

- Section 4.4.1, "Viewing a List of Pre-Configured Alarms"
- Section 4.4.2, "Viewing and Clearing Latched Alarms"
- Section 4.4.3, "Configuring an Alarm"
- Section 4.4.4, "Authentication Related Security Alarms"

Section 4.4.1

Viewing a List of Pre-Configured Alarms

To view a list of alarms pre-configured for the device, navigate to ***Diagnostic*** » ***Configure Alarms***. The **Alarms** table appears.



Alarms

access
admin

InsertRecord

Name	Level	Latch	Trap	Log	LED&Relay	Refresh Time
BPDU Guard activated	ERRO	On	On	On	On	60 s
Can't create more mcast IP groups	WARN	On	On	On	On	60 s
Clock manager alarm	WARN	On	On	On	On	60 s
Configuration changed	INFO	Off	On	On	Off	60 s
Default keys in use	WARN	On	On	On	Off	0 s
Excessive failed login attempts	WARN	On	On	On	On	60 s
GMRP cannot learn more addresses	WARN	On	On	On	On	1 s
GVRP cannot learn more VLANs	WARN	On	On	On	On	1 s
IEEE1588 alarm	WARN	On	On	On	On	60 s
Inconsistent speed/dpx in trunk	ERRO	On	On	On	On	1 s

Figure 45: Alarms Table

NOTE

This list of alarms (configurable and non-configurable) is accessible through the Command Line Interface (CLI) using the **`alarms`**. *For more information, refer to Section 2.6.1, "Available CLI Commands".*

For information about modifying a pre-configured alarm, refer toSection 4.4.3, "Configuring an Alarm".

Section 4.4.2

Viewing and Clearing Latched Alarms

To view a list of alarms that are configured to latch, navigate to ***Diagnostics*** » ***View Latched Alarms***. The **Latched Alarms** table appears.

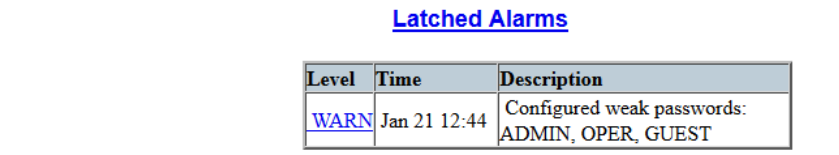


Figure 46: Latched Alarms Table

To clear the passive alarms from the list, do the following:

1. Navigate to ***Diagnostics*** » ***Clear Latched Alarms***. The **Clear Latched Alarms** form appears.

Figure 47: Clear Latched Alarms Form

1. Confirm Button

2. Click **Confirm**.

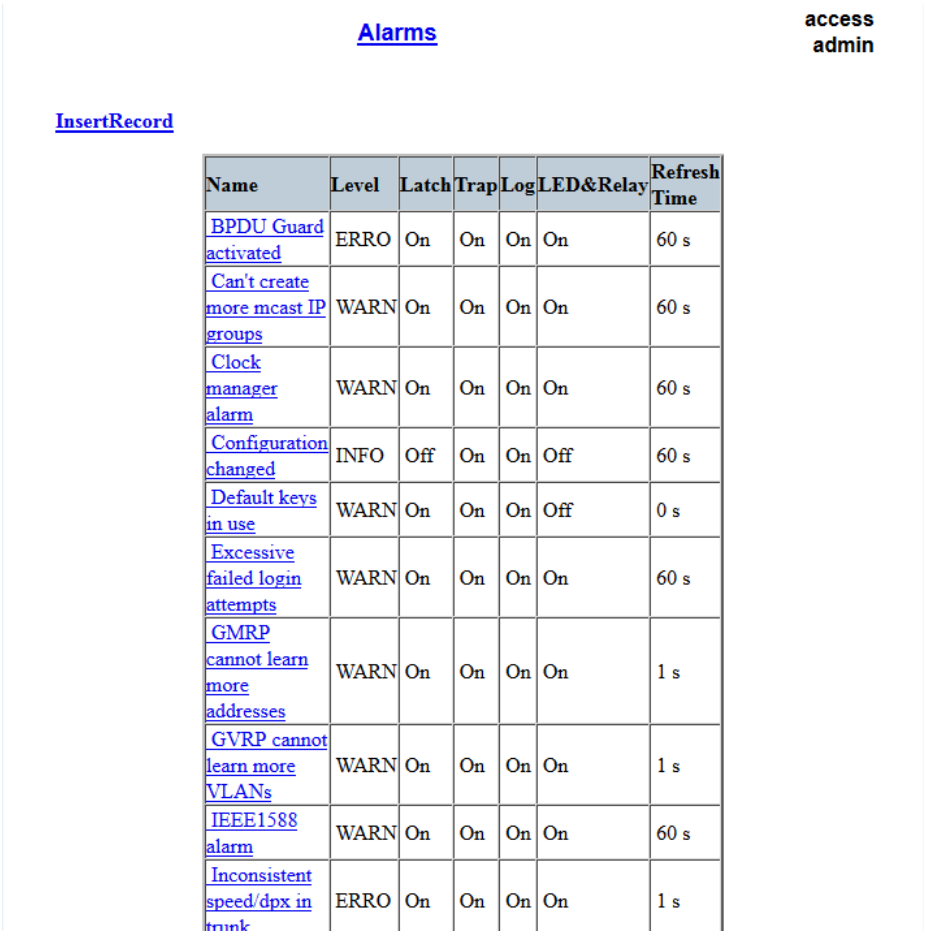
Section 4.4.3
Configuring an Alarm

While all alarms are pre-configured on the device, some alarms can be modified to suit the application. This includes enabling/disabling certain features and changing the refresh time.

To configuring an alarm, do the following:

IMPORTANT!
Critical and Alert level alarms are not configurable and cannot be disabled.

1. Navigate to ***Diagnostic*** » ***Configure Alarms***. The **Alarms** table appears.



Alarms

access
admin

InsertRecord

Name	Level	Latch	Trap	Log	LED&Relay	Refresh Time
BPDU Guard activated	ERRO	On	On	On	On	60 s
Can't create more mcast IP groups	WARN	On	On	On	On	60 s
Clock manager alarm	WARN	On	On	On	On	60 s
Configuration changed	INFO	Off	On	On	Off	60 s
Default keys in use	WARN	On	On	On	Off	0 s
Excessive failed login attempts	WARN	On	On	On	On	60 s
GMRP cannot learn more addresses	WARN	On	On	On	On	1 s
GVRP cannot learn more VLANs	WARN	On	On	On	On	1 s
IEEE1588 alarm	WARN	On	On	On	On	60 s
Inconsistent speed/dpx in trunk	ERRO	On	On	On	On	1 s

Figure 48: Alarms Table

2. Select an alarm. The **Alarms** form appears.

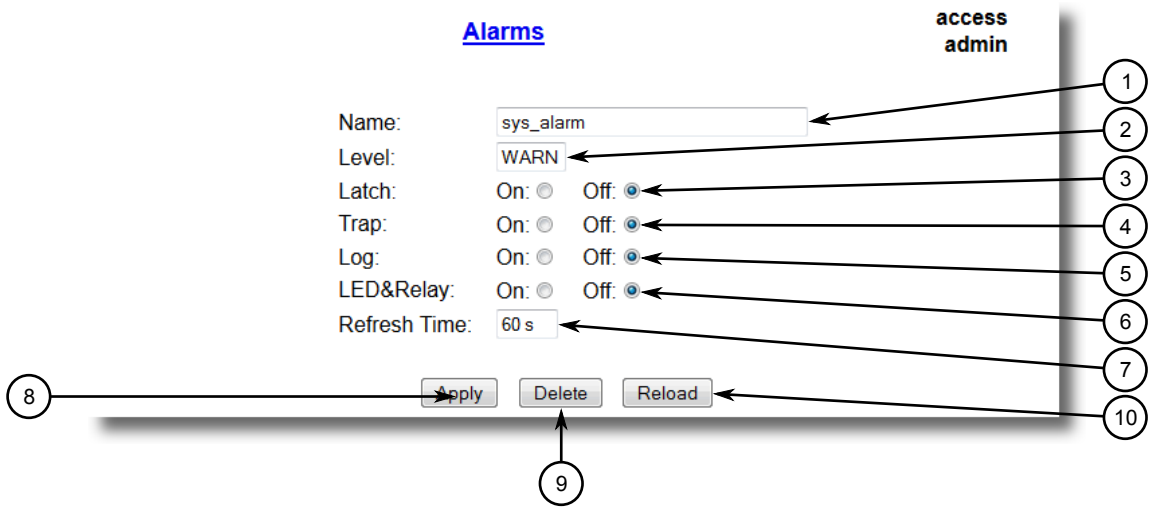


Figure 49: Alarms Form

1. Name Box **2.** Level Box **3.** Latch Box **4.** Trap Box **5.** Log Box **6.** LED & Relay Box **7.** Refresh Time Box **8.** Apply Button **9.** Delete Button **10.** Reload Button

3. Configure the following parameter(s) as required:

Parameter	Description
Name	**Synopsis:** Any 34 characters **Default:** sys_alarm The alarm name, as obtained through the **`alarms`** CLI command.
Level	**Synopsis:** { EMRG, ALRT, CRIT, ERRO, WARN, NOTE, INFO, DEBG } Severity level of the alarm: • EMERG - The device has had a serious failure that caused a system reboot. • ALERT - The device has had a serious failure that did not cause a system reboot. • CRITICAL - The device has a serious unrecoverable problem. • ERROR - The device has a recoverable problem that does not seriously affect operation. • WARNING - Possibly serious problem affecting overall system operation. • NOTIFY - Condition detected that is not expected or not allowed. • INFO - Event which is a part of normal operation, e.g. cold start, user login etc. • DEBUG - Intended for factory troubleshooting only. This parameter is not configurable.
Latch	**Synopsis:** { On, Off } **Default:** Off Enables latching occurrence of this alarm in the Alarms Table.
Trap	**Synopsis:** { On, Off } **Default:** Off Enables sending an SNMP trap for this alarm.
Log	**Synopsis:** { On, Off } **Default:** Off Enables logging the occurrence of this alarm in syslog.txt.

Parameter	Description
LED & Relay	**Synopsis:** { On, Off } **Default:** Off Enables LED and fail-safe relay control for this alarm. If latching is not enabled, this field will remain disabled.
Refresh Time	**Synopsis:** 0 s to 60 s **Default:** 60 s Refreshing time for this alarm.

4. Click **Apply**.

Section 4.4.4
Authentication Related Security Alarms

The following describes the authentication-related security messages that can be generated by ROS:

- Section 4.4.4.1, “Security Alarms for Login Authentication”
- Section 4.4.4.2, “Security Messages for Port Authentication”

Section 4.4.4.1
Security Alarms for Login Authentication

ROS provides various logging options related to login authentication. A user can log into a ROS device in three different ways: Console, SSH or Telnet. ROS can log messages in the syslog, send a trap to notify an SNMP manager, and/or raise an alarm when a successful and unsuccessful login event occurs. In addition, when a weak password is configured on a unit or when the primary authentication server for TACACS+ or RADIUS is not reachable, ROS will raise alarms, send SNMP traps and log messages in the syslog.

The following is a list of log and alarm messages related to user authentication:

- Weak Password Configured
- Login and Logout Information
- Excessive Failed Login Attempts
- RADIUS Server Unreachable
- TACACS Server Unreachable
- TACACS Response Invalid
- SNMP Authentication Failure

NOTE
All alarms and log messages related to login authentication are configurable. For more information about configuring alarms, refer to Section 4.4.3, “Configuring an Alarm”.

Weak Password Configured

ROS generates this alarm and logs a message in the syslog when a weak password is configured in the **Passwords** table.

Message Name	Alarm	SNMP Trap	Syslog
Weak Password Configured	Yes	Yes	Yes

Default Keys In Use

ROS generates this alarm and logs a message in the syslog when default keys are in use. For more information about default keys, refer to Section 1.7, “Certificate and Key Requirements”.

NOTE
For Non-Controlled (NC) versions of ROS, this alarm is only generated when default SSL keys are in use.

Message Name	Alarm	SNMP Trap	Syslog
Default Keys In Use	Yes	Yes	Yes

Login and Logout Information

ROS generates this alarm and logs a message in the syslog when a successful and unsuccessful login attempt occurs. A message is also logged in the syslog when a user with a certain privilege level is logged out from the device.

Login attempts are logged regardless of how the user accesses the device (i.e. SSH, Web, Console, Telnet or RSH). However, when a user logs out, a message is only logged when the user is accessing the device through SSH, Telnet or Console.

Message Name	Alarm	SNMP Trap	Syslog
Successful Login	Yes	Yes	Yes
Failed Login	Yes	Yes	Yes
User Logout	No	No	Yes

Excessive Failed Login Attempts

ROS generates this alarm and logs a message in the syslog after 10 failed login attempts by a user occur within a span of five minutes. Furthermore, the service the user attempted to access will be blocked for one hour to prevent further attempts.

Message Name	Alarm	SNMP Trap	Syslog
Excessive Failed Login Attempts	Yes	Yes	Yes

RADIUS Server Unreachable

ROS generates this alarm and logs a message in the syslog when the primary RADIUS server is unreachable.

Message Name	Alarm	SNMP Trap	Syslog
Primary RADIUS Server Unreachable	Yes	Yes	Yes

TACACS+ Server Unreachable

ROS generates this alarm and logs a message in the syslog when the primary TACACS+ server is unreachable.

Message Name	Alarm	SNMP Trap	Syslog
Primary TACACS Server Unreachable	Yes	Yes	Yes

TACACS+ Response Invalid

ROS generate this alarm and logs a message in the syslog when the response from the TACACS+ server is received with an invalid CRC.

Message Name	Alarm	SNMP Trap	Syslog
TACACS Response Invalid	Yes	Yes	Yes

SNMP Authentication Failure

ROS generates this alarm, sends an authentication failure trap, and logs a message in the syslog when an SNMP manager with incorrect credentials communicates with the SNMP agent in ROS.

Message Name	Alarm	SNMP Trap	Syslog
SNMP Authentication Failure	Yes	Yes	Yes

Section 4.4.4.2

Security Messages for Port Authentication

The following is the list of log and alarm messages related to port access control in ROS:

- MAC Address Authorization Failure
- Secure Port X Learned MAC Addr on VLAN X
- Port Security Violated

MAC Address Authorization Failure

ROS generates this alarm and logs a message in the syslog when a host connected to a secure port on the device is communicating using a source MAC address which has not been authorized by ROS, or the dynamically learned MAC address has exceeded the total number of MAC addresses configured to be learned dynamically on the secured port. This message is only applicable when the port security mode is set to *Static MAC*.

Message Name	Alarm	SNMP Trap	Syslog
MAC Address Authorization Failure	Yes	Yes	Yes

Secure Port X Learned MAC Addr on VLAN X

ROS logs a message in the syslog and sends a configuration change trap when a MAC address is learned on a secure port. Port X indicates the secured port number and VLAN number on that port. This message is not configurable in ROS.

Message Name	SNMP Trap	Syslog
Secure Port X Learned MAC Addr on VLAN X	Yes	Yes

Port Security Violated

This message is only applicable when the security mode for a port is set to "802.1X or 802.1X/MAC-Auth"

ROS this alarm and logs a message in the syslog when the host connected to a secure port tries to communicate using incorrect login credentials.

Message Name	Alarm	SNMP Trap	Syslog
802.1X Port X Authentication Failure	Yes	Yes	Yes
802.1X Port X Authorized Addr. XXX	No	No	Yes

Section 4.5

Managing the Configuration File

The device configuration file for ROS is a single CSV (Comma-Separate Value) formatted ASCII text file, named `config.csv`. It can be downloaded from the device to view, compare against other configuration files, or store for backup purposes. It can also be overwritten by a complete or partial configuration file uploaded to the device.

To prevent unauthorized access to the contents of the configuration file, the file can be encrypted and given a password/passphrase key.

The following sections describe how to manage the configuration file:

- Section 4.5.1, “Configuring Data Encryption”
- Section 4.5.2, “Updating the Configuration File”

Section 4.5.1

Configuring Data Encryption

To encrypt the configuration file and protect it with a password/passphrase, do the following:

NOTE
Data encryption is not available in Non-Controlled (NC) versions of ROS . When switching between Controlled and Non-Controlled (NC) versions of ROS , make sure data encryption is disabled. Otherwise, the NC version of ROS will ignore the encrypted configuration file and load the factory defaults.

NOTE
Only configuration data is encrypted. All comments and table names in the configuration file are saved as clear text.

NOTE
When sharing a configuration file between devices, make sure both devices have the same passphrase configured. Otherwise, the configuration file will be rejected.

NOTE
Encryption must be disabled before the device is returned to Siemens or the configuration file is shared with Customer Support.

IMPORTANT!
Never downgrade the ROS software version beyond ROS v4.1 when encryption is enabled. Make sure the device has been restored to factory defaults before downgrading.

1. Navigate to ***Administration » Configure Data Storage***. The **Data Storage** form appears.

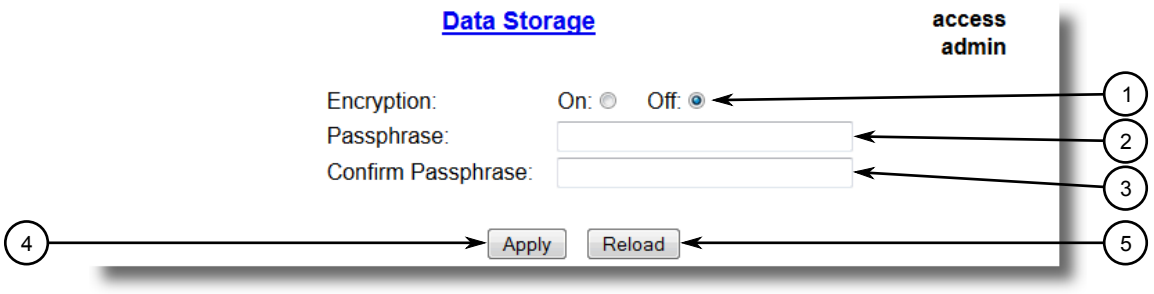


Figure 50: Data Storage Form

1. Encryption Options **2.** Passphrase Box **3.** Confirm Passphrase Box **4.** Apply Button **5.** Reload Button

2. Configure the following parameter(s) as required:

Parameter	Description
Encryption	**Synopsis:** { On, Off } Enable/disable encryption of data in configuration file.
Passphrase	**Synopsis:** 31 character ascii string This passphrase is used as a secret key to encrypt the configuration data. Encrypted data can be decrypted by any device configured with the same passphrase.
Confirm Passphrase	**Synopsis:** 31 character ascii string This passphrase is used as a secret key to encrypt the configuration data. Encrypted data can be decrypted by any device configured with the same passphrase.

3. Click **Apply**.

Section 4.5.2

Updating the Configuration File

Once downloaded from the device, the configuration file can be updated using a variety of different tools:

NOTE
For information about uploading/downloading files, refer to Section 3.5, "Uploading/Downloading Files".

- Any text editing program capable of reading and writing ASCII files
- Difference/patching tools (e.g. the UNIX *diff* and *patch* command line utilities)
- Source Code Control systems (e.g. CVS, SVN)

CAUTION!
Configuration hazard – risk of data loss. Do not edit an encrypted configuration file. Any line that has been modified manually will be ignored.

ROS also has the ability to accept partial configuration updates. For example, to update only the parameters for Ethernet port 1 and leave all other parameters unchanged, transfer a file containing only the following lines to the device:

```
# Port Parameters
ethPortCfg
Port,Name,Media,State,AutoN,Speed,Dupx,FlowCtrl,LFI,Alarm,
1,Port 1,100TX,Enabled,On,Auto,Auto,Off,Off,On,
```

Section 4.6

Managing an Authentication Server

The following sections describe how to setup and configure an authentication server:

- Section 4.6.1, “Managing RADIUS Authentication”
- Section 4.6.2, “Managing TACACS+ Authentication”

Section 4.6.1

Managing RADIUS Authentication

ROS can be configured to act as a RADIUS client and forward user credentials to a RADIUS (Remote Authentication Dial In User Service) server for remote authentication and authorization.

RADIUS is a UDP-based protocol used for carrying authentication, authorization and configuration information between a Network Access Server (NAS) that desires to authenticate its links and a shared authentication server. It provides centralized authentication and authorization for network access.

RADIUS is also widely used in conjunction with the IEEE 802.1X standard for port security using the Extensible Authentication Protocol (EAP).

NOTE
For more information about the RADIUS protocol, refer to RFC 2865.

For more information about the Extensible Authentication Protocol (EAP), refer to RFC 3748.

IMPORTANT!
RADIUS messages are sent as UDP messages. The switch and the RADIUS server must use the same authentication and encryption key.

IMPORTANT!
ROS supports both Protected Extensible Authentication Protocol (PEAP) and EAP-MD5. PEAP is more secure and is recommended if available in the supplicant.

In a RADIUS access request, the following attributes and values are typically sent by the RADIUS client to the RADIUS server:

Attribute	Value
User-Name	{ Guest, Operator, Admin }
User-Password	{ password }
Service-Type	1

Attribute	Value
Vendor-Specific	Vendor-ID: 15004 Type: 1 Length: 11 String: RuggedCom

A RADIUS server may also be used to authenticate access on ports with 802.1X security support. When this is required, the following attributes are sent by the RADIUS client to the RADIUS server:

Attribute	Value
User-Name	{ The username as derived from the client's EAP identity response }
NAS-IP-Address	{ The Network Access Server IP address }
Service-Type	2
Frame-MTU	1500
EAP-Message[a]	{ A message(s) received from the authenticating peer }

[a] *EAP-Message is an extension attribute for RADIUS, as defined by RFC 2869.*

The following sections describe how to configure RADIUS authentication:

- Section 4.6.1.1, “Configuring the RADIUS Server”
- Section 4.6.1.2, “Configuring the RADIUS Client”

Section 4.6.1.1
Configuring the RADIUS Server

The Vendor-Specific attribute (or VSA) sent to the RADIUS server as part of the RADIUS request is used to determine the access level from the RADIUS server. This attribute may be configured within the RADIUS server with the following information:

Attribute	Value
Vendor-Specific	Vendor-ID: 15004 Format: String Number: 2 Attribute: { Guest, Operator, Admin }

NOTE
If no access level is received in the response packet from the RADIUS server, access is denied.

Section 4.6.1.2
Configuring the RADIUS Client

The RADIUS client can be configured to use two RADIUS servers: a primary server and a backup server. If the primary server is unavailable, the device will automatically attempt to connect with the backup server.

NOTE
The RADIUS client uses the Password Authentication Protocol (PAP) to verify access.

To configure access to either the primary or backup RADIUS servers, do the following:

1. Navigate to ***Administration*** » ***Configure Security Server*** » ***Configure RADIUS Server***. The **RADIUS Server** table appears.

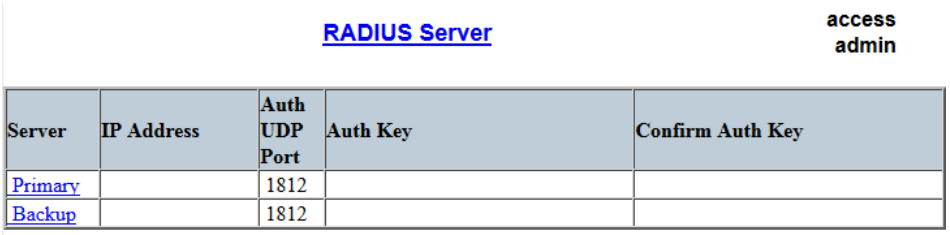


Figure 51: RADIUS Server Table

2. Select either **Primary** or **Backup** from the table. The **RADIUS Server** form appears.

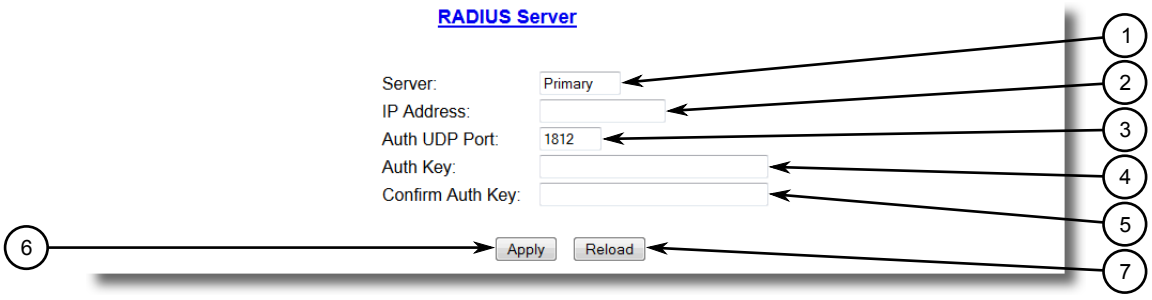


Figure 52: RADIUS Server Form

1. Server Box **2.** IP Address Box **3.** Auth UDP Port Box **4.** Auth Key Box **5.** Confirm Auth Key Box **6.** Apply Button **7.** Reload Button

3. Configure the following parameter(s) as required:

Parameter	Description
Server	**Synopsis:** Any 8 characters **Default:** Primary This field tells whether this configuration is for a Primary or a Backup Server.
IP Address	**Synopsis:** ###.###.###.### where ### ranges from 0 to 255 The Server IP Address.
Auth UDP Port	**Synopsis:** 1 to 65535 **Default:** 1812 The IP Port on server.
Auth Key	**Synopsis:** 31 character ASCII string The authentication key to be shared with server.

Parameter	Description
Confirm Auth Key	**Synopsis:** 31 character ASCII string The authentication key to be shared with server.

4. Click **Apply**.

Section 4.6.2
Managing TACACS+ Authentication

TACACS+ (Terminal Access Controller Access-Control System Plus) is a TCP-based access control protocol that provides authentication, authorization and acccounting services to routers, Network Access Servers (NAS) and other networked computing devices via one or more centralized servers.

The following sections describe how to configure TACACs+ authentication:

- Section 4.6.2.1, “Configuring TACACS+”
- Section 4.6.2.2, “Configuring User Priviliges”

Section 4.6.2.1
Configuring TACACS+

ROS can be configured to use two TACACS+ servers: a primary server and a backup server. If the primary server is unavailable, the device will automatically attempt to connect with the backup server.

To configure access to either the primary or backup TACACS+ servers, do the following:

1. Navigate to ***Administration » Configure Security Server » Configure TacPlus Server » Configure TACACS Plus Server***. The **TACACS Plus Server** table appears.

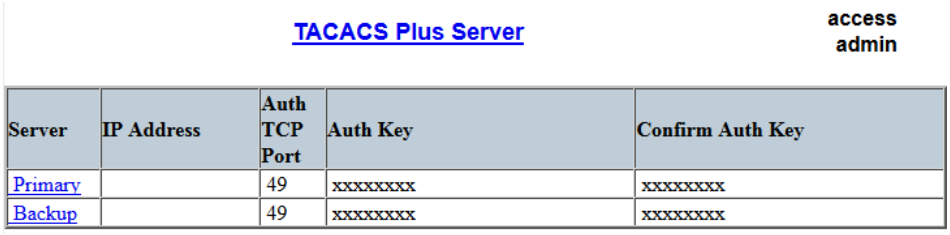


Figure 53: TACACS Plus Server Table

2. Select either **Primary** or **Backup** from the table. The **TACACS Plus Server** form appears.

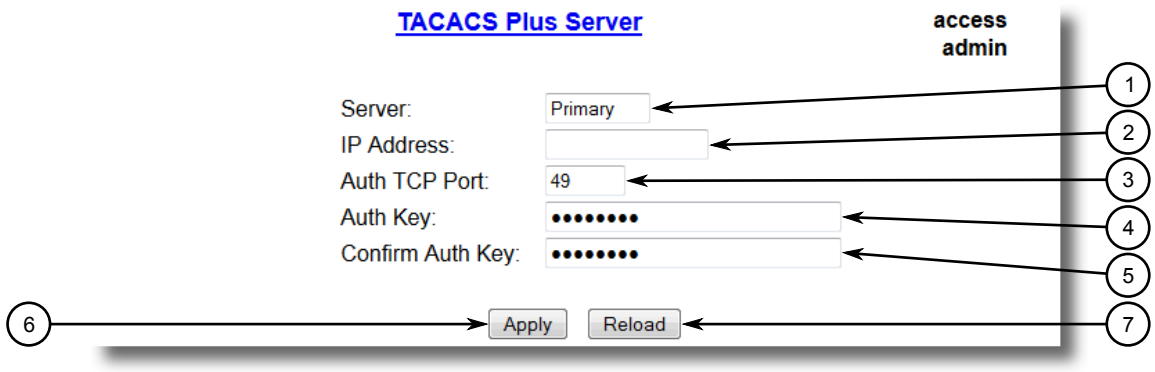


Figure 54: TACACS Plus Server Form

1. Server Box **2.** IP Address Box **3.** Auth TCP Port Box **4.** Auth Key Box **5.** Confirm Key Box **6.** Apply Button **7.** Reload Button

3. Configure the following parameter(s) as required:

Parameter	Description
Server	**Synopsis:** Any 8 characters **Default:** Primary This field tells whether this configuration is for a Primary or a Backup Server.
IP Address	**Synopsis:** ###.###.###.### where ### ranges from 0 to 255 The Server IP Address.
Auth TCP Port	**Synopsis:** 1 to 65535 **Default:** 49 The IP Port on server.
Auth Key	**Synopsis:** 31 character ascii string **Default:** mySecret The authentication key to be shared with server.
Confirm Auth Key	**Synopsis:** 31 character ascii string The authentication key to be shared with server.

4. Set the privilege levels for each user type (i.e. admin, operator and guest). For more information, refer to Section 4.6.2.2, “Configuring User Priviliges”.
5. Click **Apply**.

Section 4.6.2.2
Configuring User Priviliges

Each TACACS+ authentication request includes a *priv_lvl* attribute that is used to grant access to the device. By default, the attribute uses the following ranges:

- `15` represents the *admin* access level
- `2-14` represents the *operator* access level

- *1* represents the *guest* access level

To configure the privilege levels for each user type, do the following:

1. Navigate to ***Administration » Configure Security Server » Configure TacPlus Server » Configure TACPLUS Serv Privilege Config***. The **TACPLUS Serv Privilege Config** form appears.

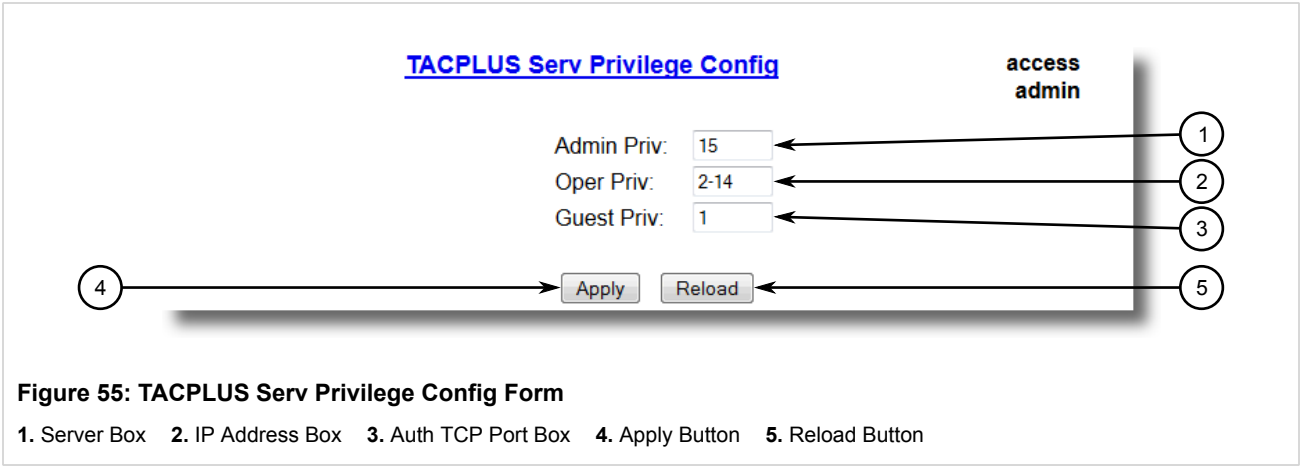


Figure 55: TACPLUS Serv Privilege Config Form

1. Server Box **2.** IP Address Box **3.** Auth TCP Port Box **4.** Apply Button **5.** Reload Button

2. Configure the following parameter(s) as required:

Parameter	Description
Admin Priv	**Synopsis:** (0 to 15)-(0 to 15) **Default:** 15 Privilege level to be assigned to the user.
Oper Priv	**Synopsis:** (0 to 15)-(0 to 15) **Default:** 2-14 Privilege level to be assigned to the user.
Guest Priv	**Synopsis:** (0 to 15)-(0 to 15) **Default:** 1 Privilege level to be assigned to the user.

3. Click **Apply**.

5 Setup and Configuration

This chapter describes how to setup and configure the device for use on a network using the various features available in ROS. It describes the following tasks:

- Section 5.1, “Managing Time Services”
- Section 5.2, “Managing SNMP”
- Section 5.3, “Managing Network Discovery”
- Section 5.4, “Managing Serial Protocols”

Section 5.1

Managing Time Services

The System Time Manager offers the following time-keeping and time synchronization features:

- Local hardware time keeping and time zone management
- SNTP (Simple Network Time Protocol) client and server

The following sections describe how to configure time-keeping and time synchronization through the System Time Manager:

- Section 5.1.1, “Configuring the Time and Date”
- Section 5.1.2, “Configuring NTP”

Section 5.1.1

Configuring the Time and Date

To set the time, date and other time-keeping related parameters, do the following:

1. Navigate to ***Administration*** » ***System Time Manager*** » ***Configure Time and Date***. The **Time and Date** form appears.

Figure 56: Time and Date Form

1. Time **2.** Date **3.** Time Zone **4.** DST Offset **5.** DST Rule **6.** Apply Button **7.** Reload Button

2. Configure the following parameter(s) as required:

Parameter	Description
Time	**Synopsis:** HH:MM:SS This parameter allows for both the viewing and setting of the local time.
Date	**Synopsis:** MMM DD, YYYY This parameter allows for both the viewing and setting of the local date.

Parameter	Description
Time Zone	**Synopsis:** { UTC-12:00 (Eniwetok, Kwajalein), UTC-11:00 (Midway Island, Samoa), UTC-10:00 (Hawaii), UTC-9:00 (Alaska), UTC-8:00 (Los Angeles, Vancouver), UTC-7:00 (Calgary, Denver), UTC-6:00 (Chicago, Mexico City), UTC-5:00 (New York, Toronto), UTC-4:30 (Caracas), UTC-4:00 (Santiago), UTC-3:30 (Newfoundland), UTC-3:00 (Brasilia, Buenos Aires), UTC-2:00 (Mid Atlantic), UTC-1:00 (Azores), UTC-0:00 (Lisbon, London), UTC+1:00 (Berlin, Paris, Rome), UTC+2:00 (Athens, Cairo, Helsinki), ... } **Default:** UTC-5:00 (New York, Toronto) This setting allows for the conversion of UTC (Universal Coordinated Time) to local time.
DST Offset	**Synopsis:** HH:MM:SS **Default:** 00:00:00 This parameter specifies the amount of time to be shifted forward/backward when DST begins and ends. For example for most part of USA and Canada, DST time shift is 1 hour (01:00:00) forward when DST begins and 1 hour backward when DST ends.
DST Rule	**Synopsis:** mm.n.d/HH:MM:SS mm.n.d/HH:MM:SS This parameter specifies a rule for time and date when the transition between Standard and Daylight Saving Time occurs. • mm - Month of the year (01 - January, 12 - December) • n - nth d-day in the month (1 - 1st d-day, 5 - 5th/last d-day) • d - day of the week (0 - Sunday, 6 - Saturday) • HH - hour of the day (0 - 24) • MM - minute of the hour (0 - 59) • SS - second of the minute (0 - 59) Example: The following rule applies in most part of USA and Canada: `03.2.0/02:00:00 11.1.0/02:00:00` DST begins on March's 2nd Sunday at 2:00am. DST ends on November's 1st Sunday at 2:00am.

Section 5.1.2
Configuring NTP

ROS may be configured to refer periodically to a specified NTP server to correct any accumulated drift in the on-board clock. ROS will also serve time via the Simple Network Time Protocol (SNTP) to hosts that request it.

Two NTP servers (primary and backup) may be configured for the device. The primary server is contacted first for each attempt to update the system time. If the primary server fails to respond, the backup server is contacted. If either the primary or backup server fails to respond, an alarm is raised.

To configure either the primary or backup NTP server, do the following:

1. Navigate to ***Administration » System Time Manager » Configure NTP Server***. The **NTP Server** table appears.

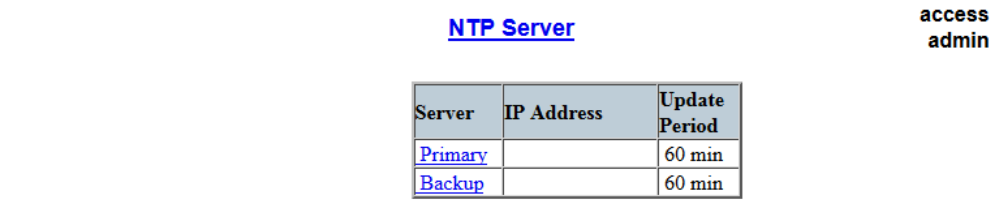


Figure 57: NTP Server Table

2. Select either **Primary** or **Backup**. The **NTP Server** form appears.

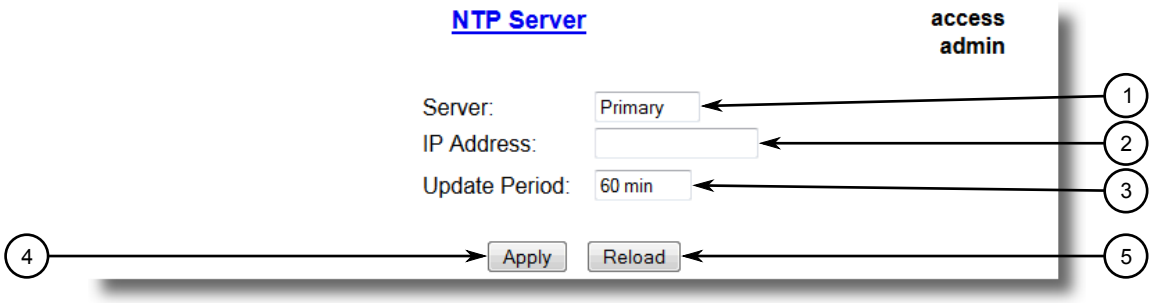


Figure 58: NTP Server Form

1. Server Box **2.** IP Address Box **3.** Update Period Box **4.** Apply Button **5.** Reload Button

3. Configure the following parameter(s) as required:

Parameter	Description
Server	**Synopsis:** Any 8 characters **Default:** Primary This field tells whether this configuration is for a Primary or a Backup Server.
IP Address	**Synopsis:** ###.###.###.### where ### ranges from 0 to 255 The Server IP Address.
Update Period	**Synopsis:** 1 to 1440 min **Default:** 60 min Determines how frequently the (S)NTP server is polled for a time update.If the server cannot be reached in three attempts that are made at one minute intervals an alarm is generated.

4. Click **Apply**.

Section 5.2
Managing SNMP

ROS supports versions 1, 2 and 3 of the Simple Network Management Protocol (SNMP), otherwise referred to as SNMPv1, SNMPv2c and SNMPv3 respectively. SNMPv3 provides secure access to the devices through a combination of authentication and packet encryption over the network. Security features for this protocol include:

Feature	Description
Message Integrity	Makes sure that a packet has not been tampered with in-transit.
Authentication	Determines if the message is from a valid source.
Encryption	Encrypts the contents of a packet to prevent it from being seen by an unauthorized source.

SNMPv3 provides security models and security levels. A security model is an authentication strategy setup for a user and the group in which the user resides. A security level is a permitted level of security within a security model. A combination of a security model and level will determine which security mechanism is employed when handling an SNMP packet.

Before configuring SNMPv3, note the following:

- Each user belongs to a group
- A group defines the access policy for a set of users
- An access policy defines what SNMP objects can be accessed for (i.e. reading, writing and creating notifications)
- A group determines the list of notifications its users can receive
- A group also defines the security model and security level for its users

For SNMPv1 and SNMPv2c, a community string can be configured. The string is mapped to the group and access level with a security name, which is configured as **User Name**.

The following sections describe how to setup and manage SNMP on the device:

- Section 5.2.1, “Managing SNMP Users”
- Section 5.2.2, “Managing Security-to-Group Mapping”
- Section 5.2.3, “Managing SNMP Groups”

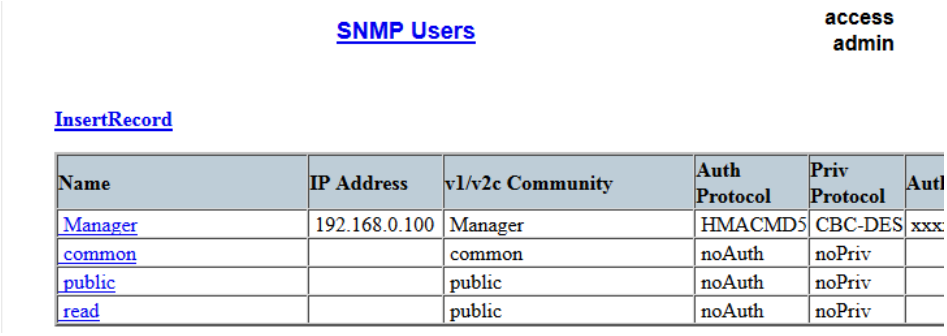
Section 5.2.1
Managing SNMP Users

The following sections describe how to configure and manage SNMP users, refer to the following:

- Section 5.2.1.1, “Viewing a List of SNMP Users”
- Section 5.2.1.2, “Adding an SNMP User”
- Section 5.2.1.3, “Deleting an SNMP User”

Section 5.2.1.1
Viewing a List of SNMP Users

To view a list of SNMP users configured on the device, navigate to ***Administration » Configure SNMP » Configure SNMP Users***. The **SNMP Users** table appears.



SNMP Users

access
admin

InsertRecord

Name	IP Address	v1/v2c Community	Auth Protocol	Priv Protocol	Auth
Manager	192.168.0.100	Manager	HMACMD5	CBC-DES	xxx
common		common	noAuth	noPriv	
public		public	noAuth	noPriv	
read		public	noAuth	noPriv	

Figure 59: SNMP Users Table

If users have not been configured, add users as needed. For more information, refer to Section 5.2.1.2, “Adding an SNMP User”.

Section 5.2.1.2
Adding an SNMP User

Multiple users (up to a maximum of 32) can be configured for the local SNMPv3 engine, as well as SNMPv1 and SNMPv2c communities.

NOTE
*When employing the SNMPv1 or SNMPv2c security level, the **User Name** parameter maps the community name with the security group and access level.*

To add a new SNMP user, do the following:

1. Navigate to ***Administration » Configure SNMP » Configure SNMP Users***. The **SNMP Users** table appears.

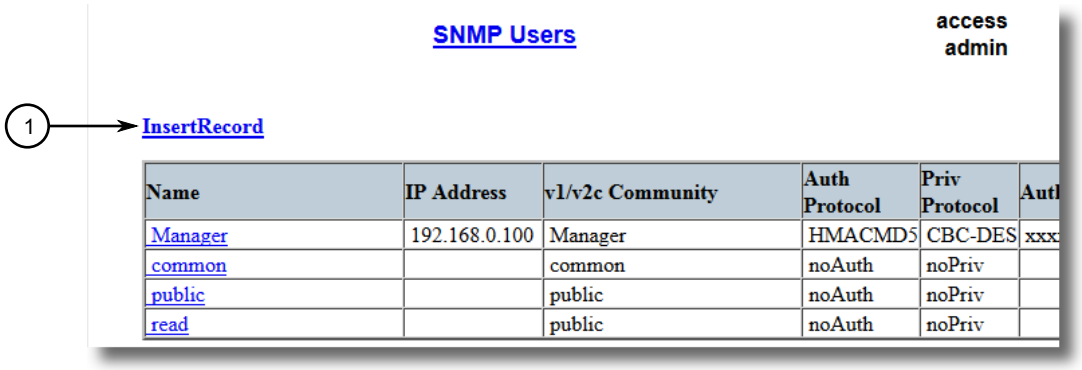


Figure 60: SNMP Users Table

1. InsertRecord

2. Click **InsertRecord**. The **SNMP Users** form appears.

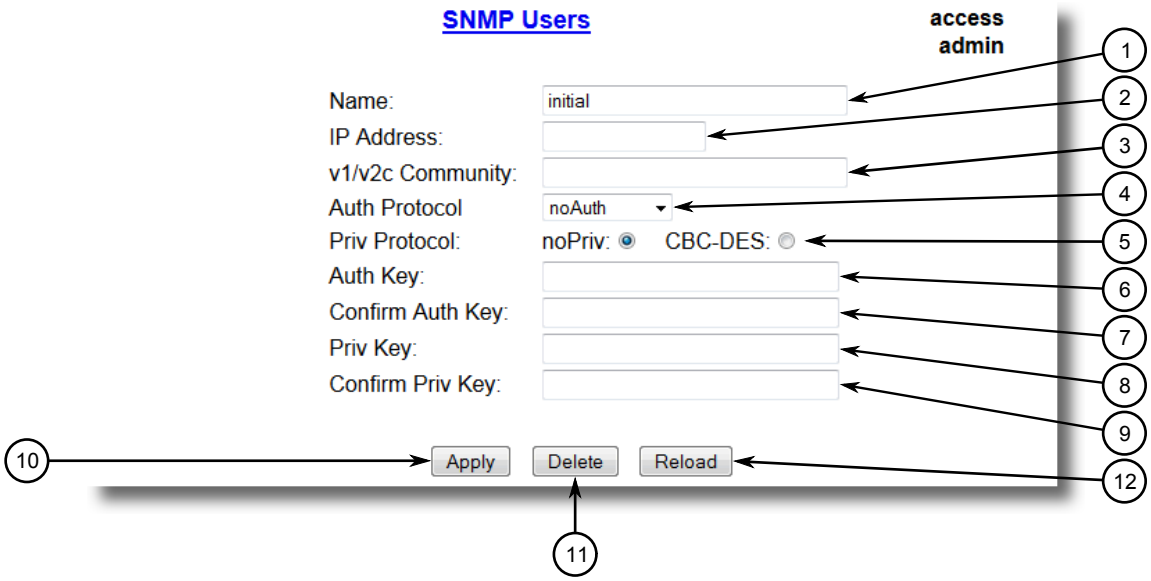


Figure 61: SNMP Users Form

1. Name Box **2.** IP Address Box **3.** v1/v2c Community Box **4.** Auth Protocol Box **5.** Priv Protocol Box **6.** Auth Key Box **7.** Confirm Auth Key Box **8.** Priv Key Box **9.** Confirm Priv Key Box **10.** Apply Button **11.** Delete Button **12.** Reload Button

NOTE

ROS requires that all user passwords meet strict guidelines to prevent the use of weak passwords. When creating a new password, make sure it adheres to the following rules:

- *Must not be less than 6 characters in length.*
- *Must not include the username or any 4 continuous alphanumeric characters found in the username. For example, if the username is Subnet25, the password may not be subnet25admin or subnetadmin. However, net25admin or Sub25admin is permitted.*

- *Must have at least one alphabetic character and one number. Special characters are permitted.*
- *Must not have more than 3 continuously incrementing or decrementing numbers. For example, Sub123 and Sub19826 are permitted, but Sub12345 is not.*

An alarm will generate if a weak password is configured. The weak password alarm can be disabled by the user. For more information about disabling alarms, refer to Section 4.4, "Managing Alarms".

3. Configure the following parameter(s) as required:

Parameter	Description
Name	**Synopsis:** Any 32 characters **Default:** initial The name of the user. This user name also represents the security name that maps this user to the security group.
IP Address	**Synopsis:** ###.###.###.### where ### ranges from 0 to 255 The IP address of the user's SNMP management station. If IP address is configured, SNMP requests from that user will be verified by IP address as well. SNMP Authentication trap will be generated to trap receivers if request was received from this user, but from any other IP address.If IP address is empty, traps can not be generated to this user, but SNMP requests will be served for this user from any IP address.
v1/v2c Community	**Synopsis:** Any 32 characters The community string which is mapped by this user/security name to the security group if security model is SNMPv1 or SNMPv2c. If this string is left empty, it will be assumed to be equal to the same as user name.
Auth Protocol	**Synopsis:** { noAuth, HMACMD5 } **Default:** noAuth An indication of whether messages sent on behalf of this user to/from SNMP engine, can be authenticated, and if so, the type of authentication protocol which is used.
Priv Protocol	**Synopsis:** { noPriv, CBC-DES } **Default:** noPriv An Indication of whether messages sent on behalf of this user to/from SNMP engine can be protected from disclosure, and if so, the type of privacy protocol which is used.
Auth Key	**Synopsis:** 31 character ASCII string The secret authentication key (password) that must be shared with SNMP client. If the key is not an emtpy string, it must be at least 6 characters long.
Confirm Auth Key	**Synopsis:** 31 character ASCII string The secret authentication key (password) that must be shared with SNMP client. If the key is not an emtpy string, it must be at least 6 characters long.
Priv Key	**Synopsis:** 31 character ASCII string The secret encription key (password) that must be shared with SNMP client. If the key is not an emtpy string, it must be at least 6 characters long.
Confirm Priv Key	**Synopsis:** 31 character ASCII string The secret encription key (password) that must be shared with SNMP client. If the key is not an emtpy string, it must be at least 6 characters long.

4. Click **Apply**.

Section 5.2.1.3
Deleting an SNMP User

To delete an SNMP user, do the following:

1. Navigate to ***Administration » Configure SNMP » Configure SNMP Users***. The **SNMP Users** table appears.

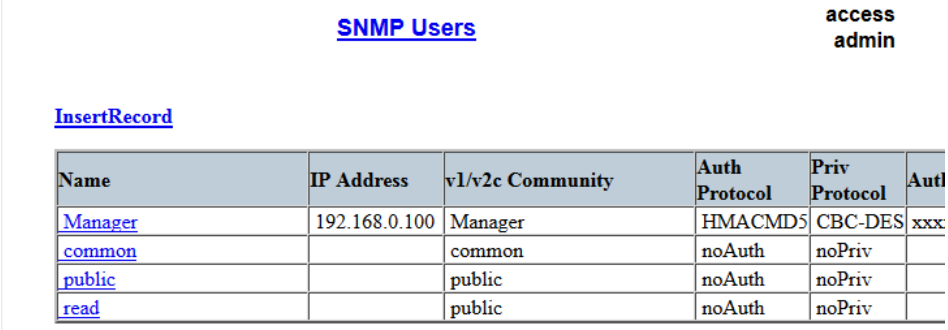


Figure 62: SNMP Users Table

2. Select the user from the table. The **SNMP Users** form appears.

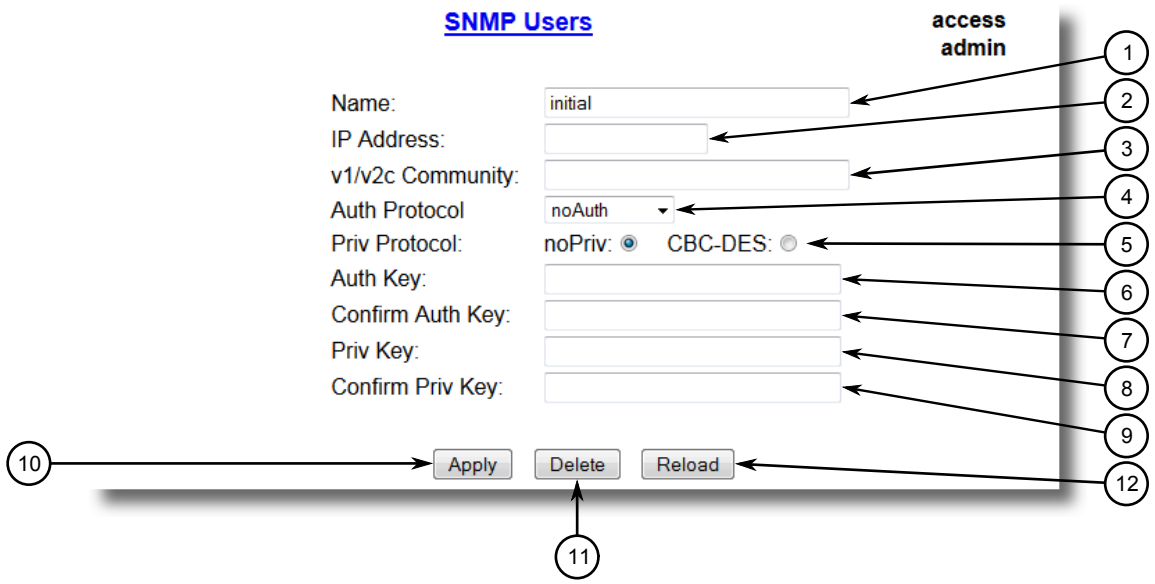


Figure 63: SNMP Users Form

1. Name Box **2.** IP Address Box **3.** v1/v2c Community Box **4.** Auth Protocol Box **5.** Priv Protocol Box **6.** Auth Key Box **7.** Confirm Auth Key Box **8.** Priv Key Box **9.** Confirm Priv Key Box **10.** Apply Button **11.** Delete Button **12.** Reload Button

3. Click **Delete**.

Section 5.2.2
Managing Security-to-Group Mapping

The following sections describe how to configure and manage security-to-group maps, refer to the following:

- Section 5.2.2.1, “Viewing a List of Security-to-Group Maps”
- Section 5.2.2.2, “Adding a Security-to-Group Map”
- Section 5.2.2.3, “Deleting a Security-to-Group Map”

Section 5.2.2.1
Viewing a List of Security-to-Group Maps

To view a list of security-to-group maps configured on the device, navigate to ***Administration » Configure SNMP » Configure SNMP Security to Group Maps***. The **SNMP Security to Group Maps** table appears.

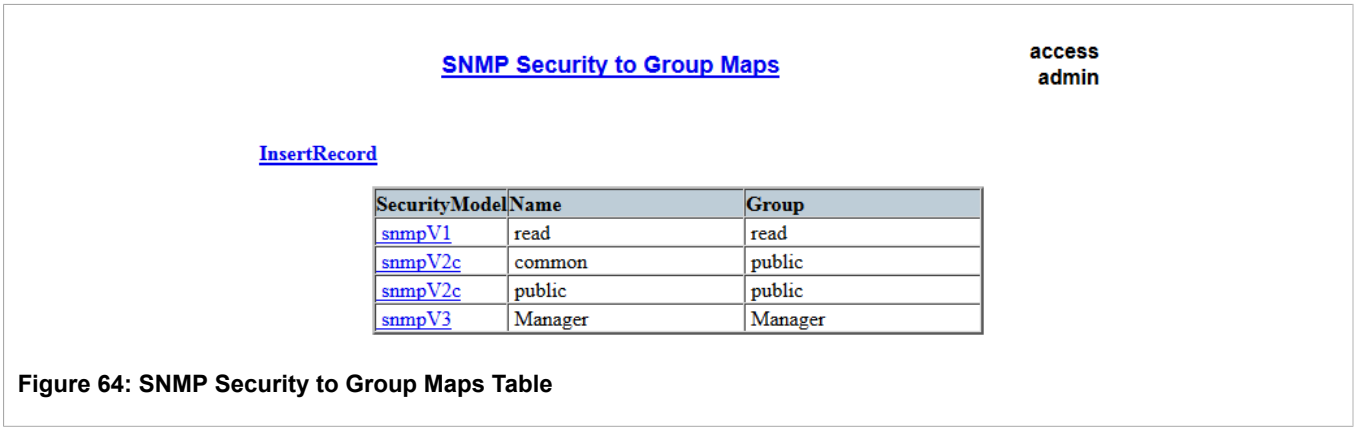


Figure 64: SNMP Security to Group Maps Table

If security-to-group maps have not been configured, add maps as needed. For more information, refer to Section 5.2.2.2, “Adding a Security-to-Group Map”.

Section 5.2.2.2
Adding a Security-to-Group Map

Multiple combinations of security models and groups can be mapped (up to a maximum of 32) for SNMP.

To add a security-to-group map, do the following:

1. Navigate to ***Administration » Configure SNMP » Configure SNMP Security to Group Maps***. The **SNMP Security to Group Maps** table appears.

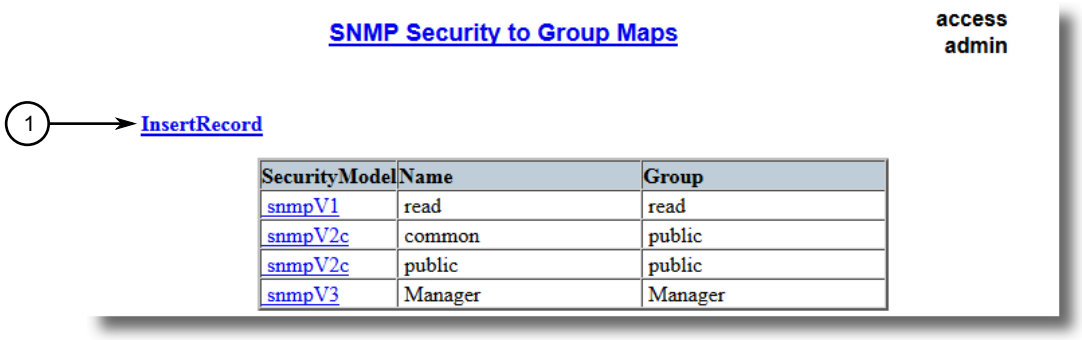


Figure 65: SNMP Security to Group Maps Table

1. InsertRecord

2. Click **InsertRecord**. The **SNMP Security to Group Maps** form appears.

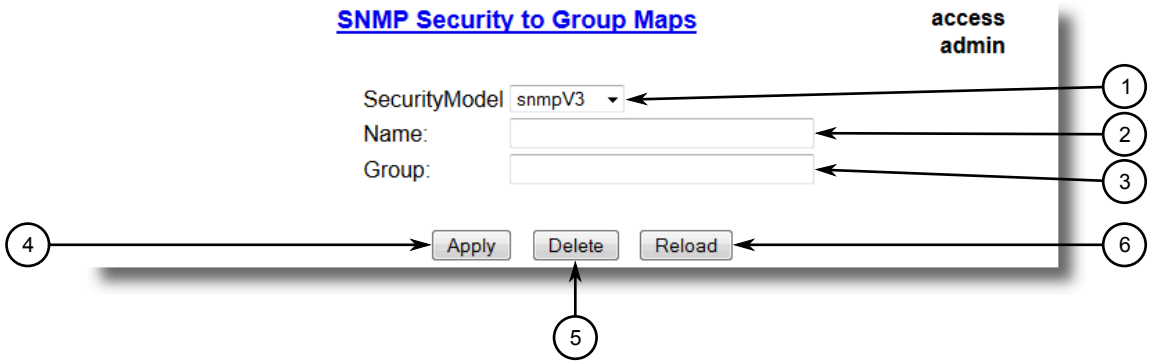


Figure 66: SNMP Security to Group Maps Form

1. Security Model Box **2.** Name Box **3.** Group Box **4.** Apply Button **5.** Delete Button **6.** Reload Button

3. Configure the following parameter(s) as required:

Parameter	Description
SecurityModel	**Synopsis:** { snmpV1, snmpV2c, snmpV3 } **Default:** snmpV3 The Security Model that provides the name referenced in this table.
Name	**Synopsis:** Any 32 characters The user name which is mapped by this entry to the specified group name.
Group	**Synopsis:** Any 32 characters The group name to which the security model and name belong. This name is used as an index to the SNMPv3 VACM Access Table.

4. Click **Apply**.

Section 5.2.2.3
Deleting a Security-to-Group Map

To delete a security-to-group map, do the following:

1. Navigate to ***Administration » Configure SNMP » Configure SNMP Security to Group Maps***. The **SNMP Security to Group Maps** table appears.

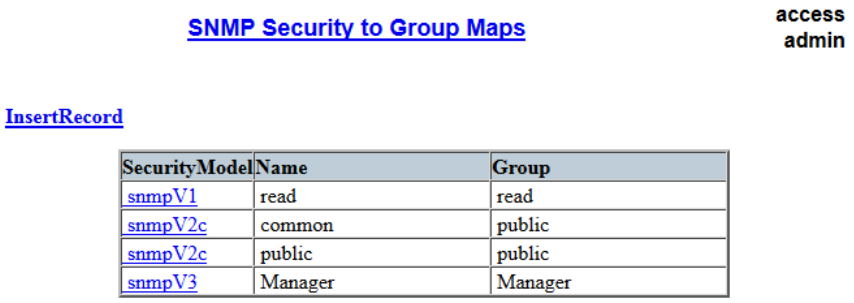


Figure 67: SNMP Security to Group Maps Table

2. Select the map from the table. The **SNMP Security to Group Maps** form appears.

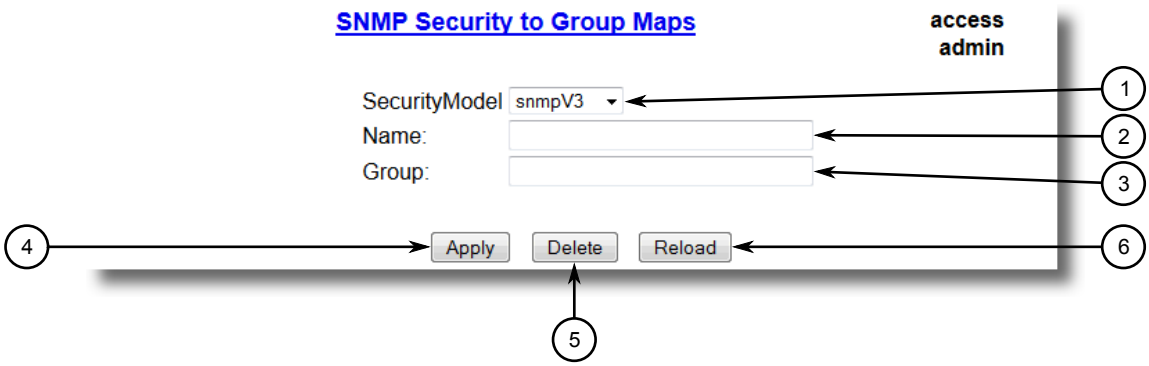


Figure 68: SNMP Security to Group Maps Form

1. Security Model Box **2.** Name Box **3.** Group Box **4.** Apply Button **5.** Delete Button **6.** Reload Button

3. Click **Delete**.

Section 5.2.3
Managing SNMP Groups

Multiple SNMP groups (up to a maximum of 32) can be configured to have access to SNMP.

The following sections describe how to configure and manage SNMP groups on the device:

- Section 5.2.3.1, “Viewing a List of SNMP Groups”
- Section 5.2.3.2, “Adding an SNMP Group”
- Section 5.2.3.3, “Deleting an SNMP Group”

Section 5.2.3.1
Viewing a List of SNMP Groups

To view a list of SNMP groups configured on the device, navigate to ***Administration*** » ***Configure SNMP*** » ***Configure SNMP Access***. The **SNMP Access** table appears.

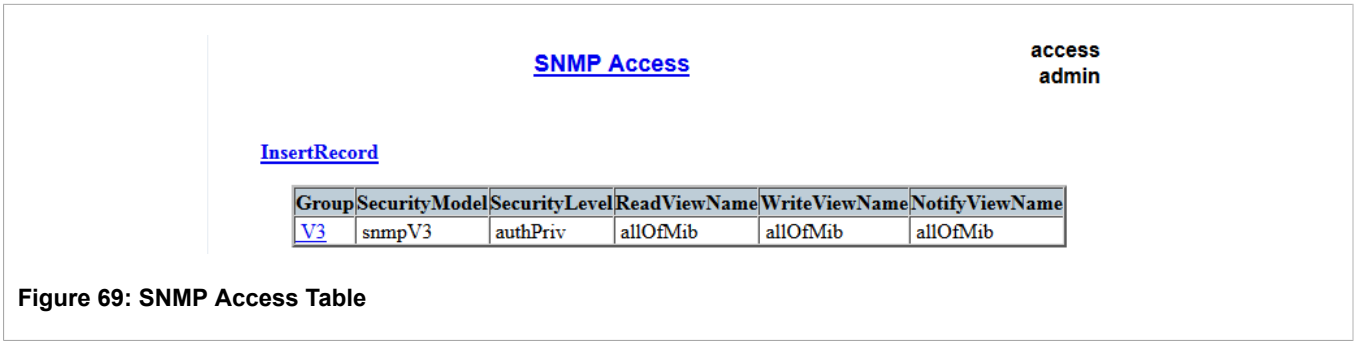


Figure 69: SNMP Access Table

If SNMP groups have not been configured, add groups as needed. For more information, refer to Section 5.2.3.2, “Adding an SNMP Group”.

Section 5.2.3.2
Adding an SNMP Group

To add an SNMP group, do the following:

1. Navigate to ***Administration*** » ***Configure SNMP*** » ***Configure SNMP Access***. The **SNMP Access** table appears.

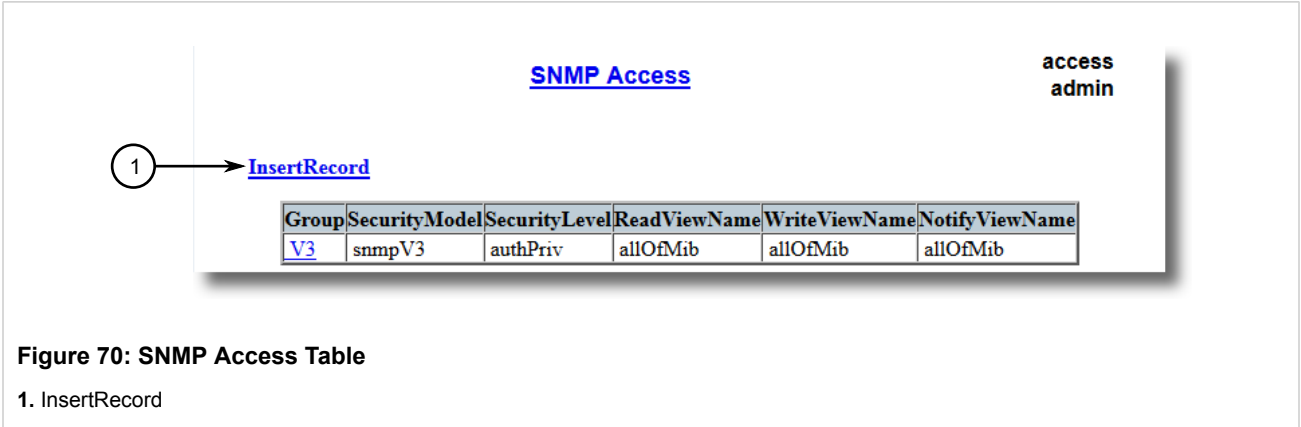


Figure 70: SNMP Access Table

1. InsertRecord

2. Click **InsertRecord**. The **SNMP Access** form appears.

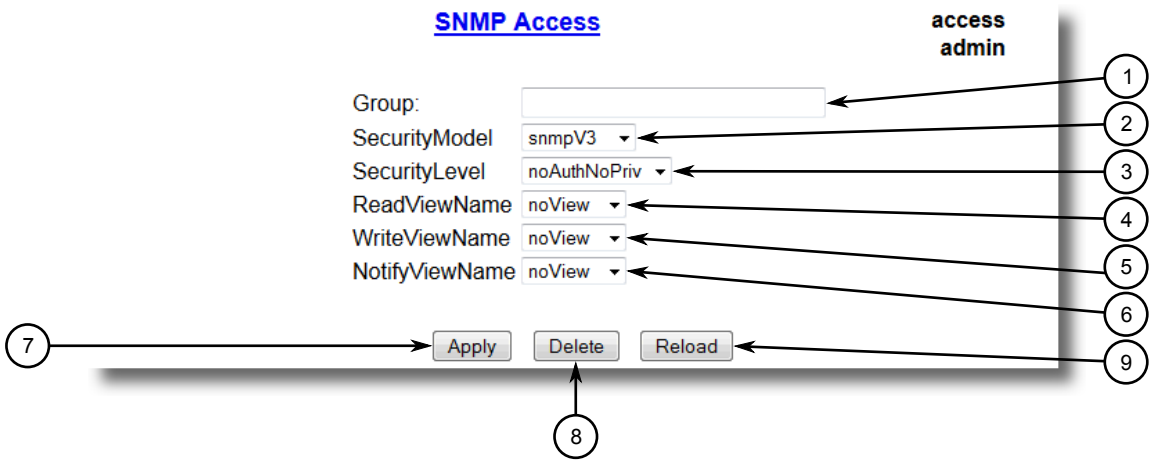


Figure 71: SNMP Access Form

1. Group Box **2.** Security Model Box **3.** Security Level Box **4.** ReadViewName Box **5.** WriteViewName Box **6.** NotifyViewName Box **7.** Apply Button **8.** Delete Button **9.** Reload Button

3. Configure the following parameter(s) as required:

Parameter	Description
Group	**Synopsis:** Any 32 characters The group name to which the security model and name belong. This name is used as an index to the SNMPv3 VACM Access Table.
SecurityModel	**Synopsis:** { snmpV1, snmpV2c, snmpV3 } **Default:** snmpV3 In order to gain the access rights allowed by this entry, configured security model must be in use.
SecurityLevel	**Synopsis:** { noAuthNoPriv, authNoPriv, authPriv } **Default:** noAuthNoPriv The minimum level of security reqwuired in order to gain the access rights allowed by this entry. A security level of noAuthNoPriv is less than authNoPriv, which is less than authPriv.
ReadViewName	**Synopsis:** { noView, V1Mib, allOfMib } **Default:** noView This parameter identifies the MIB tree(s) to which this entry authorizes read access. If the value is noView, then no read access is granted.
WriteViewName	**Synopsis:** { noView, V1Mib, allOfMib } **Default:** noView This parameter identifies the MIB tree(s) to which this entry authorizes write access. If the value is noView, then no write access is granted.
NotifyViewName	**Synopsis:** { noView, V1Mib, allOfMib } **Default:** noView This parameter identifies the MIB tree(s) to which this entry authorizes access for notifications. If the value is noView, then no access for notifications is granted.

4. Click **Apply**.

Section 5.2.3.3
Deleting an SNMP Group

To delete an SNMP group, do the following:

1. Navigate to ***Administration » Configure SNMP » Configure SNMP Access***. The **SNMP Access** table appears.

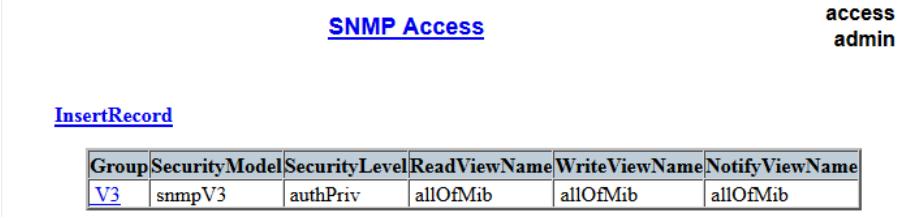


Figure 72: SNMP Access Table

2. Select the group from the table. The **SNMP Access** form appears.

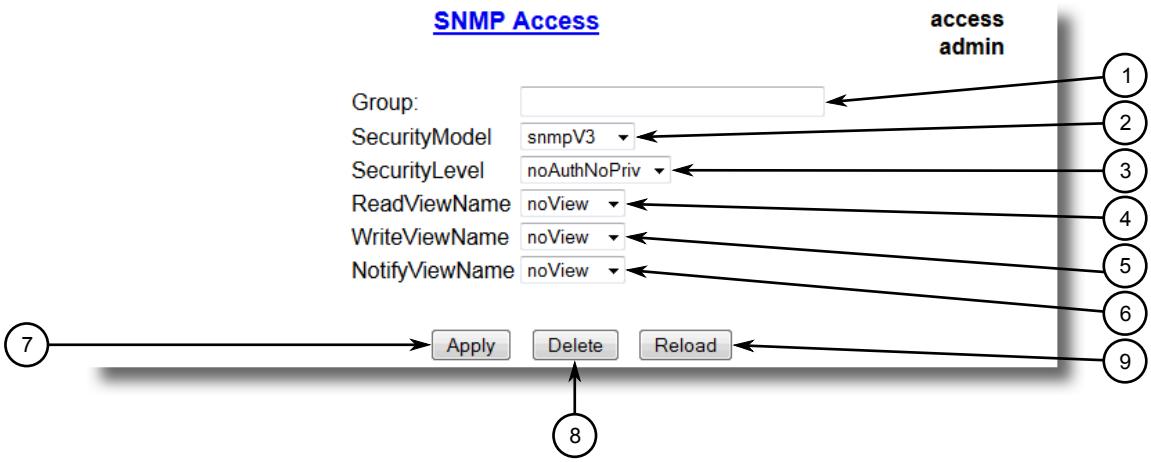


Figure 73: SNMP Access Form

1. Group Box **2.** Security Model Box **3.** Security Level Box **4.** ReadViewName Box **5.** WriteViewName Box **6.** NotifyViewName Box **7.** Apply Button **8.** Delete Button **9.** Reload Button

3. Click **Delete**.

Section 5.3
Managing Network Discovery

ROS supports the RUGGEDCOM Discovery Protocol (RCDP), a Layer 2 protocol for automated network discovery.

RUGGEDCOM Discovery Protocol (RCDP) supports the deployment of ROS -based devices that have not been configured since leaving the factory. ROS devices that have not been configured all have the default IP (Layer 3) address. Connecting more than one of them on a Layer 2 network means that one cannot use standard IP-based

configuration tools to configure them. The behavior of IP-based mechanisms such as the web interface, SSH, telnet, or SNMP will all be undefined.

Since RCDP operates at Layer 2, it can be used to reliably and unambiguously address multiple devices even though they may share the same IP configuration.

Siemens 's RUGGEDCOM Explorer is a lightweight, standalone Windows application that supports RCDP. It is capable of discovering, identifying and performing basic configuration of ROS-based devices via RCDP. The features supported by RCDP include:

- Discovery of ROS-based devices over a Layer 2 network.
- Retrieval of basic network configuration, ROS version, order code, and serial number.
- Control of device LEDs for easy physical identification.
- Configuration of basic identification, networking, and authentication parameters.

For security reasons, RUGGEDCOM Explorer will attempt to disable RCDP on all devices when Explorer is shut down. If RUGGEDCOM Explorer is unable to disable RCDP on a device, ROS will automatically disable RCDP after approximately one hour of inactivity.

NOTE
RCDP is not compatible with VLAN-based network configurations. For correct operation of RUGGEDCOM Explorer, no VLANs (tagged or untagged) must be configured. All VLAN configuration items must be at their default settings.

NOTE
ROS responds to RCDP requests only. It does not under any circumstances initiate any RCDP-based communication.

To enable or disable RCDP, do the following:

1. Navigate to ***Network Discovery*** » ***Configure RCDP Parameters***. The **RCDP Parameters** form appears.

Figure 74: RCDP Parameters Form

1. RCDP Discovery Options **2.** Apply Button **3.** Reload Button

2. Select **Enabled** to enable RCDP, or select **Disabled** to disable RCDP.
3. Click **Apply**.

Section 5.4

Managing Serial Protocols

ROS supports the use of numerous serial protocols to control serial port communication.

Serial interface bit rates can be configured in the range of 100 to 230400 bps. A *turnaround* time is supported to enforce minimum times between successive messages transmitted via a serial port.

CAUTION!
Configuration hazard – risk of communication disruption. Changing the ID for the management VLAN will break any active Raw Socket TCP connections. If this occurs, reset all serial ports.

NOTE
To transport protocol messages through the network, either TCP/IP or UDP/IP transport can be used. The exception is the TCPModbus protocol, which cannot be employed over UDP.

NOTE
The setting of Differentiated Services Code Point (DSCP) in the IP header is provided for TCP/IP and UDP/IP transport in the egress direction only.

NOTE
Debugging facilities include statistics and tracing information on a serial port and/or network transport.

ROS supports the following serial protocols:

Protocol	Features
Raw Socket	• Transport streams of characters from one serial port to another over an IP network • XON/XOFF flow control • Configurable local and remote IP port numbers per serial port • Many-to-many UDP transactions • TCP accept or request connection mode • Point-to-point TCP connection mode and a broadcast connection mode, in which up to 64 remote servers may connect to a central server • Packetization and sending data on a specific packet size, a specific character, or up on a timeout • Configurable *turnaround* time to enforce minimum time between messages sent out the serial port
DNP Over Raw Socket	• Packetization and sending data per the DNP v3.0 protocol specification
Preemptive Raw Socket	• Transport streams of characters from one serial port to another over an IP network • XON/XOFF flow control for a permanent connection • Configurable local and remote IP port numbers per serial port • TCP accept or request one permanent connection on a configured IP address • TCP accept one dynamic connection from a different IP address • Dynamic connection activity timer controlled • Packetization triggered by a specific packet size, a specific character, or a timeout for each connection
Modbus	• Operation in TCPModbus Server Gateway or Client Gateway mode • Multi-master mode on the server • Configurable behavior for sending exceptions • Full control over packetization timers • A configurable Auxiliary IP port number for applications that do not support port 502
DNP	• Packetization per the protocol specification • CRC checking in message headers received from the serial port • Local and remote source address learning
Microlok	• Packetization per the protocol specification

Protocol	Features
WIN	• Packetization per the protocol specification • CRC checking in message headers received from the serial port
TIN	• Support for two TIN protocol modes • Packetization per the protocol specification • CRC checking in message headers received from the serial port • Remote source address learning, specific for the two different modes
Telnet Com Port	• Raw Socket protocol with additional support for the serial break signal • Compliant with RFC2217 [http://tools.ietf.org/html/rfc2217]

The following sections describe how to configure and manage serial protocols:

- Section 5.4.1, “Encapsulation Concepts”
- Section 5.4.2, “Modbus Concepts”
- Section 5.4.3, “DNP, Microlok, TIN and WIN Concepts”
- Section 5.4.4, “Force Half-Duplex (HD) Operation Mode”
- Section 5.4.5, “Configuring a Serial Port”
- Section 5.4.6, “Configuring the Raw Socket Protocol”
- Section 5.4.7, “Configuring the Preemptive Raw Socket Protocol”
- Section 5.4.8, “Configuring a TCP Modbus Server”
- Section 5.4.9, “Configuring a TCP Modbus Client”
- Section 5.4.10, “Configuring the WIN and TIN Protocols”
- Section 5.4.11, “Configuring the MicroLok Protocol”
- Section 5.4.12, “Configuring the DNP Protocol”
- Section 5.4.13, “Configuring the DNP Over Raw Socket Protocol”
- Section 5.4.14, “Configuring the Mirrored Bits Protocol”
- Section 5.4.15, “Configuring the Telnet Com Port Protocol”
- Section 5.4.16, “Managing Raw Socket Remote Hosts”
- Section 5.4.17, “Managing Device Addresses”
- Section 5.4.18, “Viewing the TIN Dynamic Address Table”
- Section 5.4.19, “Viewing Statistics for Serial Protocol Links”
- Section 5.4.20, “Viewing Statistics for Serial Protocol Connections”
- Section 5.4.21, “Viewing Serial Port Statistics”
- Section 5.4.22, “Clearing Statistics for Specific Serial Ports”
- Section 5.4.23, “Resetting Serial Ports”

Section 5.4.1

Encapsulation Concepts

The following sections describe some of the concepts related to encapsulation and the implementation of serial protocols in ROS:

- Section 5.4.1.1, “Raw Socket Character Encapsulation”
- Section 5.4.1.2, “RTU Polling”
- Section 5.4.1.3, “Broadcast RTU Polling”
- Section 5.4.1.4, “Preemptive Raw Socket”
- Section 5.4.1.5, “Port Redirectors”
- Section 5.4.1.6, “Message Packetization”

Section 5.4.1.1
Raw Socket Character Encapsulation

Character encapsulation is used any time a stream of characters must be reliably transported across a network.

Character streams can be created by any type of device. The baud rates supported at either server need not be the same. If configured, the server will obey XON/XOFF flow control from the end devices.

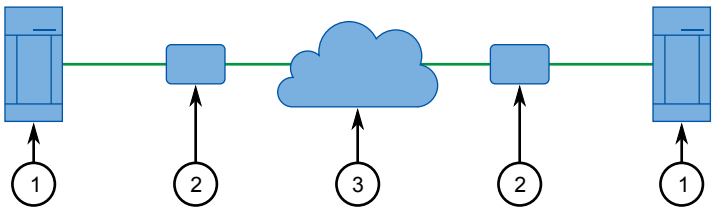


Figure 75: Character Encapsulation

1. Server **2.** RMC30 **3.** Ethernet

Section 5.4.1.2
RTU Polling

Remote Terminal Unit (RTU) polling applies to a variety of RTU protocols, including Modbus ASCII and DNP.

NOTE
If a given device or service employs a serial protocol that is supported by ROS , it is advised to configure ROS to use that particular protocol, rather than another one (e.g. RawSocket) that can be made to be (partly) compatible.

Host equipment may connect directly to a server via a serial port, may use a port redirection package, or may connect natively to the (Ethernet/IP) network.

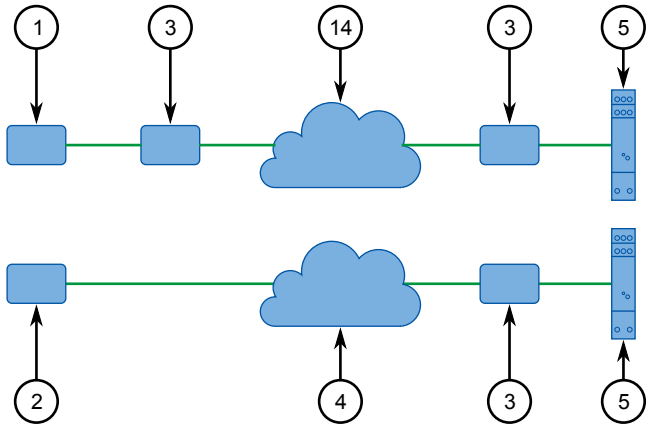


Figure 76: RTU Polling

1. Host **2.** Host with Port Redirection Software **3.** RMC30 **4.** Ethernet **5.** RTU

If a server is used at the host end, it will wait for a request from the host, encapsulate it in an IP Datagram and send it to the remote side. There, the remote server will forward the original request to the RTU. When the RTU replies, the server will forward the encapsulated reply back to the host end.

The server maintains configurable timers to help decide if replies and requests are complete.

The server also handles the process of line-turnaround when used with RS485. It is important to note that unsolicited messages from RTUs in half-duplex mode cannot be supported reliably. Message processing time includes sending a message over RS485, a packtimer and a turnaround time. To handle half-duplex mode reliably, the turnaround time must be configured long enough to allow an expected response to be received. Any other messages will not be sent to the RS485 line within the processing time. If such a message is received from the network, it will be delayed. It is up to the application to handle polling times on ports properly.

Section 5.4.1.3

Broadcast RTU Polling

Broadcast polling allows a single host-connected server to distribute a polling stream to a number of remote Remote Terminal Units (RTUs).

The host equipment connects via a serial port to a server. Up to 64 remote servers may connect to the host server via the network.

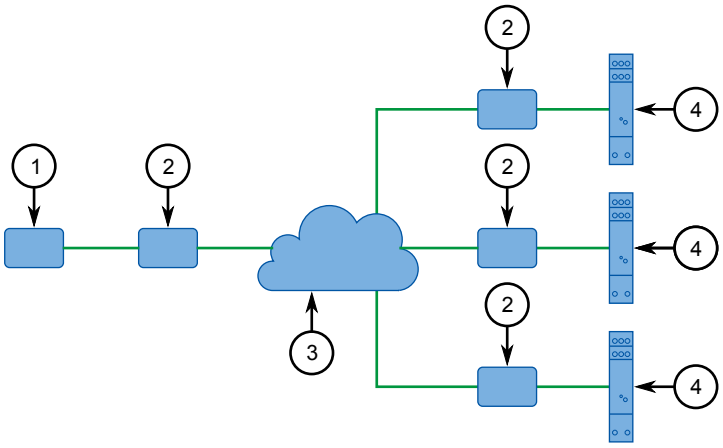


Figure 77: Broadcast RTU Polling

1. Host **2.** RMC30 **3.** Ethernet **4.** RTU

Initially, the remote servers establish connections with the host server. The host server is configured to accept a maximum of three incoming connections.

The host sequentially polls each RTU. Each poll received by the host server is forwarded (i.e. broadcast) to all of the remote servers. All RTUs receive the request and the appropriate RTU issues a reply. The reply is returned to the host server, where it is forwarded to the host.

Section 5.4.1.4

Preemptive Raw Socket

Most SCADA protocols are master/slave and support only a single master device. Preemptive Raw Socket offers the ability to have multiple masters communicate to Remote Terminal Units (RTUs) or Intelligent Electronic Devices (IEDs) in a protocol-independent manner. For example, the SCADA master polling device is the normal background process collecting data from the RTUs/IEDs on a permanent TCP connection. Occasionally, RTU/IED maintenance configuration or control may be required from a different master (on a dynamic TCP connection).

This feature allows a dynamic master to automatically preempt a permanent master. A connection request from the dynamic master would cause the permanent master to be suspended. Either closing the dynamic connection or timing out on data packets causes the permanent master session to be resumed.

The illustrates the scenario where all RTUs are connected to Preemptive Raw Socket ports of RMC30 devices.

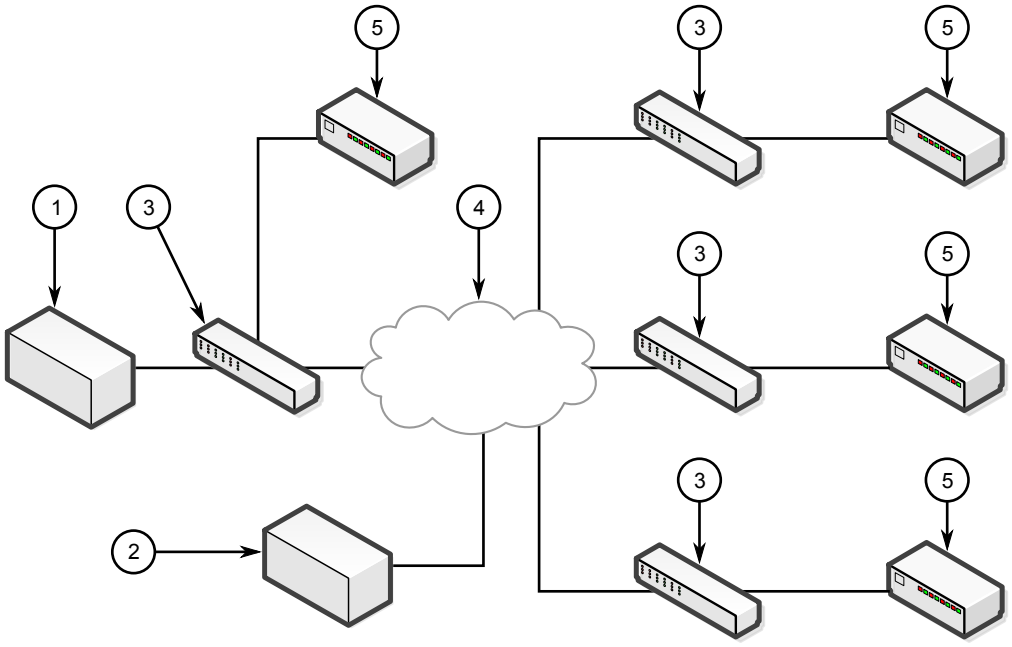


Figure 78: Permanent and Dynamic Master Connection Support

1. Permanent Master (Polling RTUs) **2.** Dynamic Master **3.** RMC30 **4.** Ethernet **5.** RTU

The permanent master is connected to the Raw Socket port of the RMC30. Raw Socket is configured to be connected to all Preemptive Raw Socket ports where polled RTUs are connected (multiple incoming connection). Preemptive Raw Socket configuration on all ports connected to RTUs will point to that Raw Socket as a permanent master (IP address and Remote IP port).

A dynamic master can establish a connection to any Preemptive Raw Socket port at any time and temporarily suspend the polling process (until the dynamic connection is cleared or times out).

Section 5.4.1.5

Port Redirectors

Port redirectors refer to software packages that emulate the existence of serial communications ports. The redirector software creates and makes these *virtual* serial ports available, providing access to the network via a TCP connection.

When a software package uses one of the virtual serial ports, a TCP connection request is sent to a remote IP address and IP port that have been programmed in to the redirector. Some redirectors also offer the ability to accept connection requests.

The Raw Socket protocol is the one most frequently used on the RMC30 for connection to serial port redirection software. The Telnet Com Port protocol may be used in place of Raw Socket if the redirection software on the other end of the connection also supports the serial break command, as defined in RFC 2217. In Telnet Com Port mode, a serial break received from the remote RFC 2217 compatible client will be transmitted as a serial break on the configured serial port, and a break signal received on the serial port will be transmitted as an RFC 2217 compatible break signal to the remote client. Note that a break signal on a serial port is defined as a condition where the serial data signal is in *space* or logic zero state for longer than the time needed to transmit one whole character, including start and stop bits.

Section 5.4.1.6
Message Packetization

The serial server buffers received characters into packets to improve network efficiency and demarcate messages.

The server uses three methods to decide when to packetize and forward the buffered characters to the network:

- Packetize on a specific character
- Packetize on timeout
- Packetize on a specific packet size

If configured to packetize on a specific character, the server will examine each received character and will packetize and forward upon receiving the configured character. The character is usually a <CR> or an <LF> character, but may be any 8 bit (0 to 255) value.

If configured to packetize on a timeout, the server will wait for a configurable time after receiving a character before packetizing and forwarding. If another character arrives during the waiting interval, the timer is restarted. This method allows characters transmitted as part of an entire message to be forwarded to the network in a single packet, when the timer expires after receiving the very last character of the message.

NOTE
Some polling software packages that perform well under DOS have been known to experience problems when used with Windows-based software or port redirection software. If the operating system does not expedite the transmission of characters in a timely fashion, pauses in transmission can be interpreted as the end of a message. Messages can be split into separate TCP packets. A locally attached server or a port redirector could packetize and forward the message incorrectly. Solutions include tuning the operating system to prevent the problem or increasing the packetizing timer.

Finally, the server will always packetize and forward on a specific packet size, specifically when the number of characters received from the serial port reaches a configured value.

Section 5.4.2
Modbus Concepts

The following sections describe some of the concepts related to Modbus and the implementation of serial protocols in ROS:

- Section 5.4.2.1, “Modbus Server Client Applications”
- Section 5.4.2.2, “Modbus TCP Performance Determinants”
- Section 5.4.2.3, “Turnaround Delay”

Section 5.4.2.1
Modbus Server Client Applications

Modbus Server and Client applications are used to transport Modbus requests and responses across IP networks.

The Modbus Client application accepts Modbus polls from a master and determines the IP address of the corresponding Remote Terminal Unit (RTU). The client then encapsulates the message in Transmission Control Protocol (TCP), respecting the Modbus TCP protocol, and forwards the frame to a Server Gateway or native Modbus TCP RTU. Returning responses are stripped of their TCP headers and issued to the master.

The Modbus Server application accepts TCP encapsulated Modbus TCP messages from Client Gateways and native masters. After removing the TCP headers, the messages are issued to the RTU. Responses are TCP encapsulated and returned to the originator.

The following illustrates a complex network of Client Gateways, Server Gateways and native TCPModbus devices.

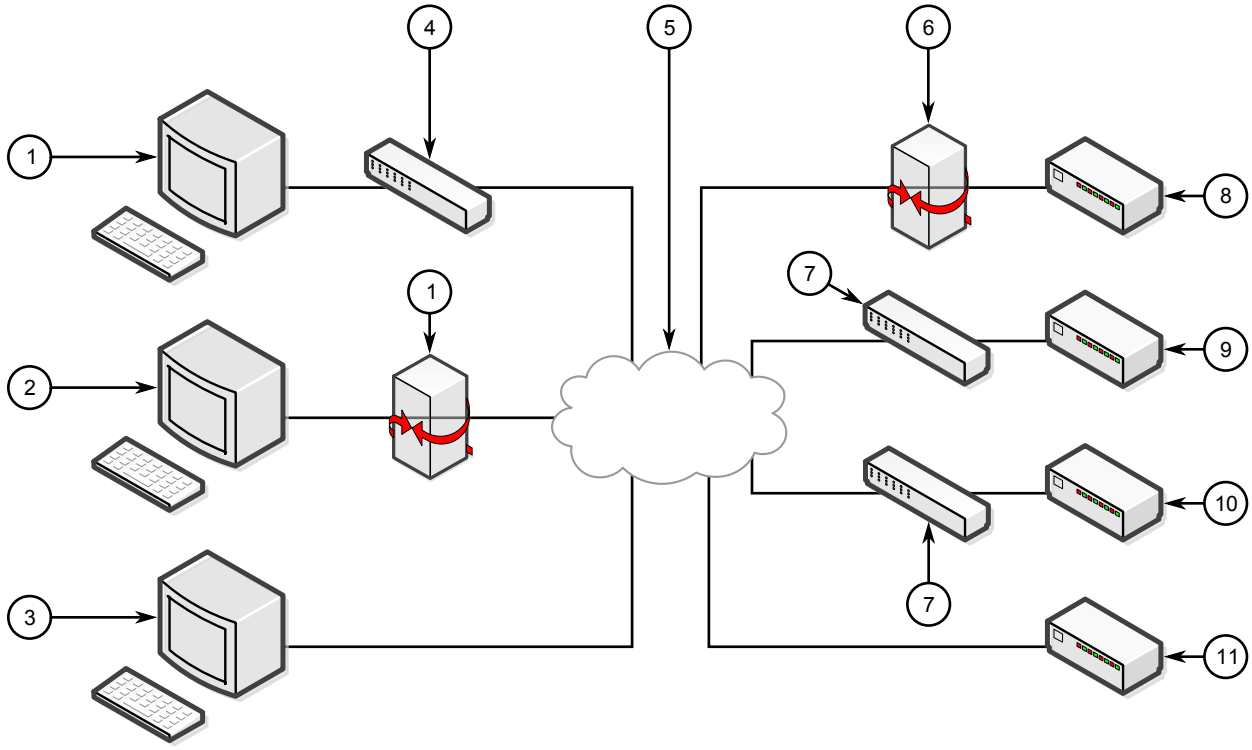


Figure 79: Modbus Client and Server

1. Master (Polling RTUs 1 and 2) **2.** Master (Polling RTUs 1, 2 and 4) **3.** Native Modbus TCP Master (Polling All RTUs) **4.** RMC30 Client Gateway **5.** RUGGEDCOM Media Converter Client Gateway **6.** Ethernet **7.** RUGGEDCOM Media Converter Server Gateway **8.** RMC30 Server Gateway **9.** RTU 1 **10.** RTU 2 **11.** RTU 3 **12.** RTU 4

Section 5.4.2.2

Modbus TCP Performance Determinants

The following illustrates the possible sources of delay and error in an end-to-end Modbus TCP exchange.

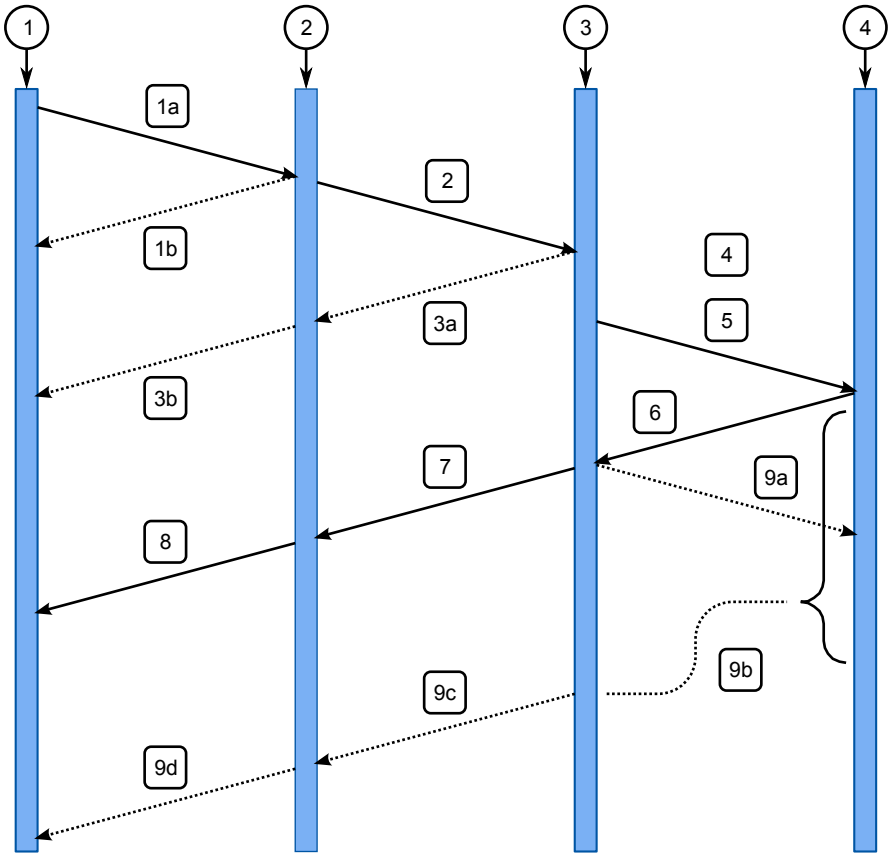


Figure 80: Sources of Delay and Error in an End-to-End Exchange

1. Master **2.** Client Gateway **3.** Server Gateway **4.** Remote Terminal Unit (RTU)

In step 1a, the master issues a request to the Client Gateway. If the Client Gateway validates the message, it will forward it to the network as step 2.

The Client Gateway can respond immediately in certain circumstances, as shown in step 1b. When the Client Gateway does not have a configuration for the specified RTU, it will respond to the master with an exception using Modbus TCP exception code 11 ("No Path"). When the Client Gateway has a configured RTU but the connection is not yet active, it will respond to the master with an exception using Modbus TCP exception code 10 ("No Response"). If the forwarding of Modbus TCP exceptions is disabled, the client will not issue any responses.

Steps 3a and 3b represent the possibility that the Server Gateway does not have a configuration for the specified RTU. The Server Gateway will always respond with a type 10 ("No Path") in step 3a, which the client will forward in step 3b.

Step 4 represents the possibility of a queuing delay. The Server Gateway may have to queue the request while it awaits the response to a previous request. The worst case occurs when a number of requests are queued for an RTU that has gone off-line, especially when the server is programmed to retry the request upon failure.

Steps 5-8 represent the case where the request is responded to by the RTU and is forwarded successfully to the master. It includes the "think time" for the RTU to process the request and build the response.

Step 9a represents the possibility the RTU is off-line, the RTU receives the request in error or that the Server Gateway receives the RTU response in error. The Server Gateway will issue an exception to the originator. If sending exceptions has not been enabled, the Server Gateway will not send any responses.

Section 5.4.2.3
Turnaround Delay

The Modbus protocol uses the concept of a *turnaround delay* in conjunction with broadcast messages. When the host sends a broadcast message (that does not invoke an RTU response), it waits for a turnaround delay time. This delay makes sure the RTU has enough time to process the broadcast message before it receives the next poll.

When polling is performed over TCP, network delays may cause the broadcast and next poll to arrive at the remote server at the same time. Configuring a turnaround delay at the server will enforce a minimum separation time between each message transmitted via the serial port.

Note that turnaround delays do not need to be configured at the host computer side and may be disabled there.

Section 5.4.3
DNP, Microlok, TIN and WIN Concepts

The following sections describe some of the concepts related to Distributed Network Protocol (DNP), Microlok, TIN and Wireless Intelligent Network (WIN) as they relate to the implementation of serial protocols in ROS:

- Section 5.4.3.1, “DNP, Microlok, TIN and WIN Applications”
- Section 5.4.3.2, “The Concept of Links”
- Section 5.4.3.3, “Address Learning for TIN”
- Section 5.4.3.4, “Address Learning for DNP”
- Section 5.4.3.5, “Broadcast Messages”
- Section 5.4.3.6, “Transport Protocols”

Section 5.4.3.1
DNP, Microlok, TIN and WIN Applications

RMC30 supports a variety of protocols that specify source and destination addresses. A destination address specifies which device should process the data, and the source address specifies which device sent the message. Having both destination and source addresses satisfies at least one requirement for peer-to-peer communication because the receiver knows where to direct responses. Each device supporting one of these protocols must have a unique address within the collection of devices sending and receiving messages to and from each other.

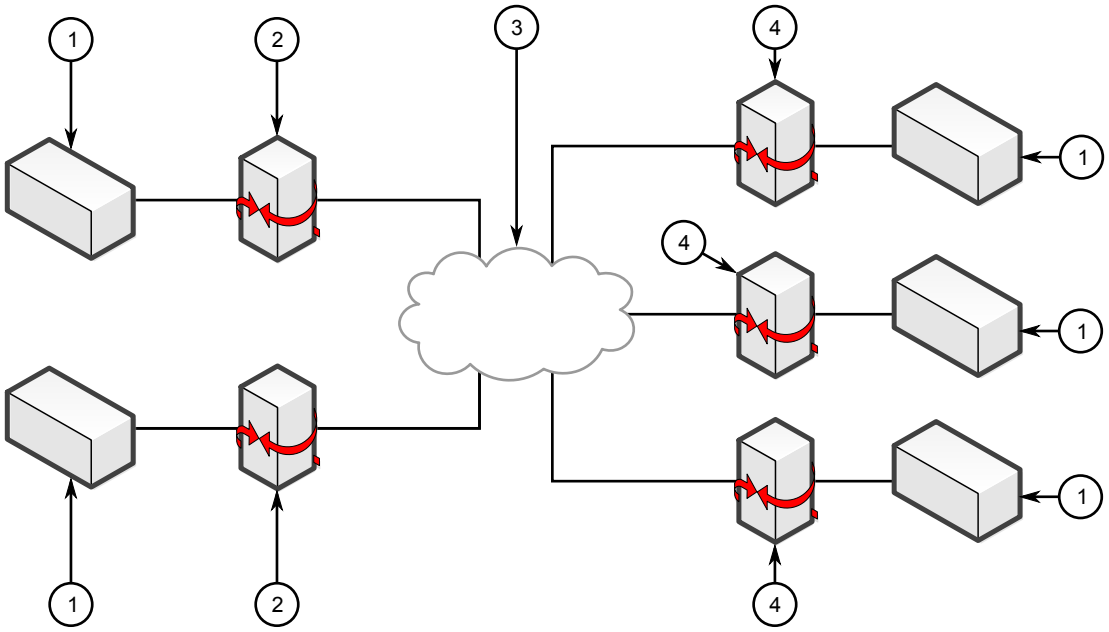


Figure 81: Source/Destination Two-Way Communication

1. Device 1 **2.** RMC30 Client Gateway **3.** Ethernet **4.** RMC30 Server Gateway

Even if the protocol can distinguish between the server and client sides, ROS does not. Both sides need to know where on the network a given destination device is. If a message is received from the network, the destination address must point to the serial port on the receiving server. If a message is received from the local serial port, the destination address must point to the IP address of the server where the addressed device is connected.

Section 5.4.3.2
The Concept of Links

A communication link is established between two IP addresses. The addressing is described below:

- The *remote address* is the source IP address in a message received over the network, and also the destination address of a message received from a serial port and transmitted on the network.
- The *local address* is the destination IP address in a message received over the network, and also the source address of a message received from a serial port and transmitted on the network.

For each link, a statistical record will be available to the user if link statistics collection is enabled in the protocol configuration.

Section 5.4.3.3
Address Learning for TIN

Address learning is implemented for the TIN protocol and learned entries are viewable in the TIN Dynamic Device Address Table. For more information about viewing the Dynamic Device Address Table Section 5.4.18, “Viewing the TIN Dynamic Address Table”.

Address Learning for TIN Mode 1

When a message with an unknown source address is received from the IP network, it is learned on the IP address and IP port. If a message with the same source address is received from another IP address and/or IP port, the address will be relearned.

The aging time will be reset whenever a unicast TIN message is received from a particular source address.

The address will be removed from the table when the aging time expires.

Address Learning for TIN Mode 2

When a message with an unknown source address is received from the IP network, it is learned on the IP address. If a message with the same source address is received from another IP address and/or IP port, it will be learned again, and another entry will be created in the Dynamic Device Address Table (TIN addresses will be duplicated).

Aging time will be reset whenever a unicast TIN message is received from a particular source address.

The address will be removed from the table when the aging time expires.

Section 5.4.3.4

Address Learning for DNP

For the DNP protocol, both the local and remote concepts of address learning are implemented. Source addresses are learned from messages received from the network for specific IP Addresses. Source addresses from messages received from the serial ports are learned for specific local serial ports.

Although the DNP protocol can be configured for TCP or UDP transport, UDP transport is used during the address learning phase as it supports all types of IP addresses: unicast, multicast and broadcast.

When a message with an unknown source address is received from the local serial port, the address is learned on that port and the local IP address.

When a message with an unknown source address is received from the IP network, on IP interface that is configured as learning interface, it is learned on the IP address of the sender and serial port is unknown.

When a message with an unknown destination address is received from a serial port, a UDP broadcast datagram is transmitted on the UDP port configured for the DNP protocol. The IP interface that transmits this broadcast is the one configured as the learning interface.

When a message with an unknown destination address is received from the IP network, it is sent to all DNP serial ports.

All learned addresses will be kept in the Device Address Table until they are active. They will also be saved in non-volatile memory and recovered if the device reboots, so the learning process does not have to be repeated because of, for example, an accidental power interruption.

The aging timer is reset whenever a message is received or sent to the specified address.

This concept makes the DNP protocol configurable with the minimum number of parameters: an IP port, a learning IP interface and an aging timer.

Section 5.4.3.5

Broadcast Messages

DNP Broadcast Messages

Addresses 65521 through 65535 are DNP 3.0 broadcast addresses. ROS supports broadcasts sending messages with those destination addresses received from serial ports to all IP Addresses found in the Device Address Table (either learned or statically configured). When a DNP broadcast message is received from the IP network, it will be distributed to all ports configured to support the DNP protocol.

TIN Broadcast Messages

TIN broadcast messages can be received only from devices connected to the serial ports.

TIN Mode 1 Broadcast Messages

These messages will be sent to all TIN Address/Ports found in the Dynamic Address Table.

TIN Mode 2 Broadcast Messages

These messages will be sent according to the configuration: to all TIN addresses on every IP address found in the Dynamic Address Table and/or to all Wayside Data Radio IP addresses found in the Static Device Address Table.

Section 5.4.3.6

Transport Protocols

For supported protocols, with exception of Modbus, either UDP datagram or TCP connection packets can be used to transport protocol data over the IP network. The Modbus data can be transported only using TCP connection, following Modbus TCP protocol. UDP supports all the addressing modes of IP – unicast, multicast and broadcast. Therefore, if address learning is enabled, UDP broadcasts will be sent across the network.

Transport for Raw Socket

The TCP transport for RawSocket requires configuration of connection request direction, remote IP address, and IP port for listening or requesting outgoing TCP connections. Only one outgoing connection can be requested, but up to 64 connections can be accepted if the port is configured to listen to incoming connection requests. For ports configured to request connections and to listen to incoming connection requests, only one connection can become active.

ROS will attempt to connect periodically if the first attempt fails and after a connection is broken.

ROS can be used to connect to any device supporting TCP (e.g. a host computer's TCP stack or a serial application on a host using port redirection software).

If Raw Socket ports are configured to use UDP for transport, up to 64 remote hosts can communicate with devices connected to local serial ports. Data in UDP packets from remote hosts configured to communicate with a particular serial port will be forwarded to that port, as long as the serial port is configured to listen on the UDP port to which the remote hosts are transmitting. Data received from the serial port will be forwarded to all remote hosts configured to communicate with that serial port.

The Raw Socket mechanism transparently passes data. It does not attempt to determine where to demarcate packets in the data received from connected devices. Given this transparency, any protocol can be encapsulated within Raw Socket.

Transport for Protocols with Defined Links

All protocols with defined links (source and destination addresses are part of protocol) can use either TCP or UDP to transport data.

The Device Address Table contains addresses and locations of devices configured (or learned) for specific protocols.

If a protocol is configured to use TCP to transport data, the server will start listening to the IP Port configured for the protocol. At the same time, TCP connections will be placed to all IP addresses where devices for that protocol are attached. ROS will keep only one connection open to one IP Address on one IP Port.

Use of Differentiated Services Code Point (DSCP)

ROS has the ability to set the DS byte in the IP header of outbound IP packets. The value can be configured on an ingress serial port, and/or for a protocol. Which value will be used depends on the protocol configured on a port and the transport configured for the particular protocol.

UDP/IP transport supports a DSCP setting per serial port or per protocol. If a configuration contains a DSCP setting per serial port as well as per protocol then the system will use whichever setting has a higher DSCP value.

TCP/IP transport supports per protocol DSCP setting. RawSocket and Modbus Server protocol properties are configured per port as well, so they always support DSCP setting per serial port.

Section 5.4.4

Force Half-Duplex (HD) Operation Mode

A *force half-duplex* mode of operation allows use of extensions to create echo loops, similar for example to an optical loop topology that utilizes the RUGGEDCOM RMC20 repeat mode function.

NOTE
If a port is set to force half-duplex mode, all data received while data is being sent will be discarded. To set this mode, the port must work natively in full-duplex mode.

The following illustrates a topology that utilizes the RMC20 repeat mode function.

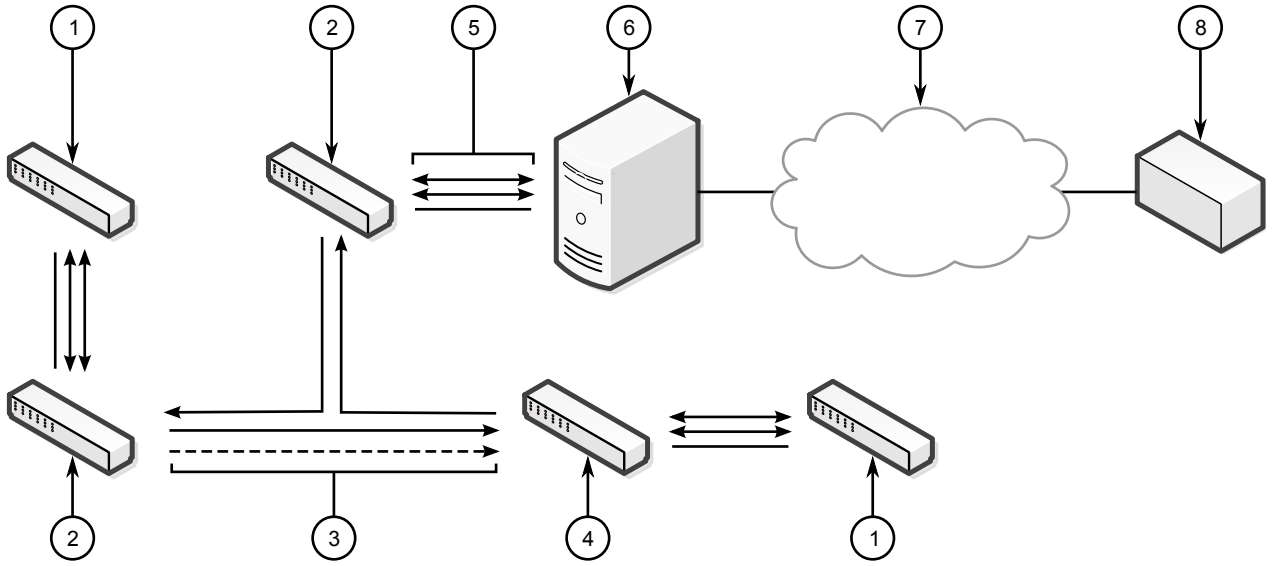


Figure 82: Optical Loop Topology

1. RS485 Slave with Repeat On **2.** RMC20 **3.** Multiple RMC20s **4.** RMC20 in Force Half-Duplex Mode **5.** RS232/422 with Repeat On **6.** RUGGEDCOM Server **7.** Ethernet **8.** RS485 Master

The repeat function will optically retransmit any data received on the optical receiver, in addition to any connected serial devices. As a result, any data transmitted from the master will be retransmitted optically to all the slaves.

This topology can be used for RS232, RS485, or RS422 multi-drop networks. In all cases, all slaves have the repeat function (DIP position 4) ON, while the one connected to the RUGGEDCOM RMC30 is configured with the repeat function OFF. The port used on the RMC30 must be in full-duplex mode, while the `ForceHD` (Force Half-Duplex) parameter must be turned ON.

Section 5.4.5

Configuring a Serial Port

To configure a serial port, do the following:

1. Navigate to ***Serial Protocols*** » ***Configure Serial Ports***. The **Serial Ports** table appears.

Serial Ports

access admin

Port	Name	Protocol	Type	ForceHD	Baud	Data Bits	Stop	Parity	Turnaround	PostTx Delay	Hold Time
1	Port 1	None	RS485	N/A	9600	8	1	None	0 ms	15 bits	Off
2	Port 2	None	RS485	N/A	9600	8	1	None	0 ms	15 bits	Off
3	Port 3	None	RS485	N/A	9600	8	1	None	0 ms	15 bits	Off
4	Port 4	None	RS485	N/A	9600	8	1	None	0 ms	15 bits	Off

Figure 83: Serial Ports Table

2. Select a serial port. The **Serial Ports** form appears.

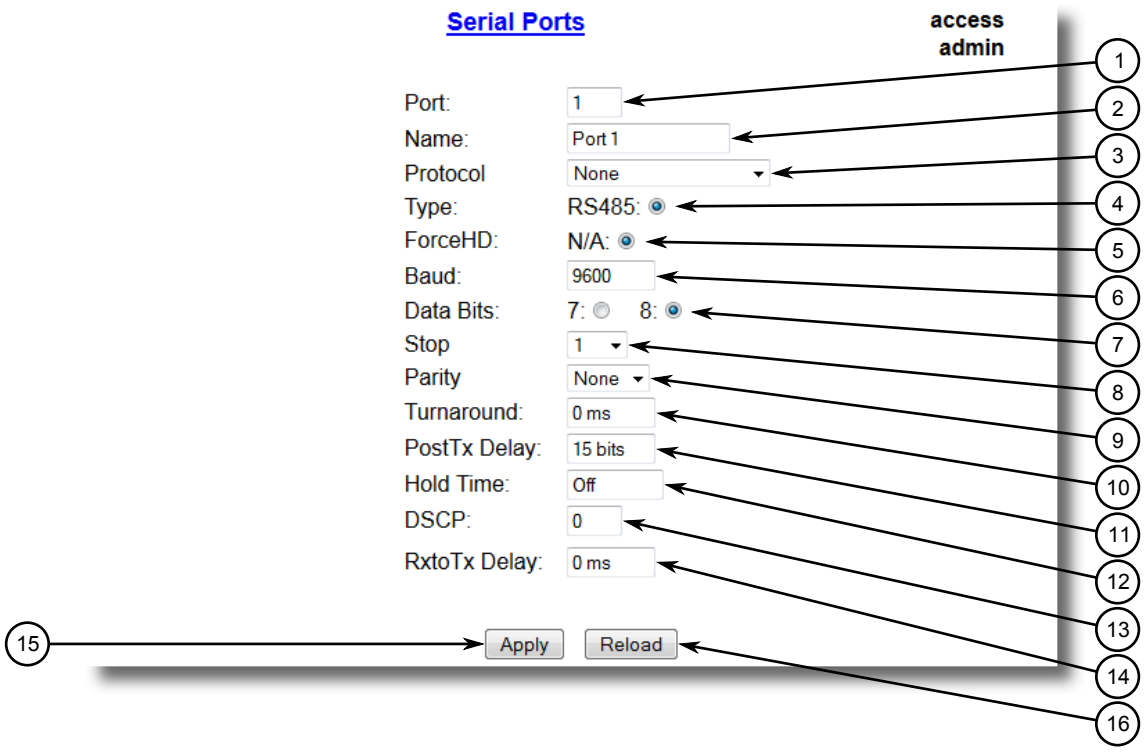


Figure 84: Serial Ports Form

1. Port Box **2.** Name Box **3.** Protocol List **4.** Type List **5.** ForceHD Options **6.** Baud Box **7.** Data Bits Options **8.** Stop List **9.** Parity List **10.** Turnaround Box **11.** PostTx Delay Box **12.** Hold Time Box **13.** DSCP Box **14.** RxtoTx Delay Box **15.** Apply Button **16.** Reload Button

3. Configure the following parameter(s) as required:

Parameter	Description
Port	**Synopsis:** 1 to maximum port number **Default:** 1 The port number as seen on the front plate silkscreen of the switch.
Name	**Synopsis:** Any 15 characters **Default:** Port 1 A descriptive name that may be used to identify the device connected on that port.
Protocol	**Synopsis:** { None, RawSocket, ModbusServer, ModbusClient, DNP, DNPRS, WIN, TIN, MicroLok, MirroredBits, PreemptRawSocket, TelnetComPort } **Default:** None The serial protocol supported on this serial port.
Type	**Synopsis:** { RS232, RS485, RS422 } **Default:** RS232 The serial port interface type.
ForceHD	**Synopsis:** { On, Off } **Default:** Off

Parameter	Description
	Enables forcing half-duplex mode of operation. While sending data out of the serial port, all received data are ignored. This mode of operation is available only on ports that operate in full-duplex mode.
Baud	**Synopsis:** 100 to 230400 **Default:** 9600 The baud rate at which to operate the port.
Data Bits	**Synopsis:** { 7, 8 } **Default:** 8 The number of data bits to operate the port with.
Stop	**Synopsis:** { 1, 1.5, 2 } **Default:** 1 The number of stop bits to operate the port with.
Parity	**Synopsis:** { None, Even, Odd } **Default:** None The parity to operate the port with.
Turnaround	**Synopsis:** 0 to 1000 **Default:** 0 ms The amount of delay (if any) to insert between the transmissions of individual messages via the serial port. For Modbus protocol this value must be non-zero. It represents the delay between sending a brodcast message and the next poll out of the serial port. Because RTUs do not reply to a broadcast, enough time must be ensured to process it.
PostTX Delay	**Synopsis:** 0 to 15 **Default:** 15 bits The number of data bits needed to generate required delay with configured baudrate after the last bit of the packet was sent out before serial UART starts listening to the RX line. This value is relevant for RS485 interfaces only.
Hold Time	**Synopsis:** 1 to 15000 ms or { off } **Default:** off The maximum amount of time, in milliseconds, that the serial packet can be held in the queue before being sent to the serial line. Time is measured from the moment the packet is received from the IP layer.
DSCP	**Synopsis:** 0 to 63 **Default:** 0 Sets the DS byte in the IP header. DS byte setting is supported in the egress direction only.
RXtoTX Delay	**Synopsis:** 0 ms to 1000 ms **Default:** 0 ms The minimum amount of time, in milliseconds, that the transmission of a new message delays after the last message is received through the serial port. This parameter is especially useful for half duplex transmission modes, such as the two-wire RS485 serial protocol. It provides the connected device with time to turn off its transmitter and to turn on its receiver, helping to ensure that the device receives the next message without data loss.

4. Click **Apply**.

Section 5.4.6

Configuring the Raw Socket Protocol

To configure the Raw Socket protocol for a serial port, do the following:

1. Make sure the serial port is configured to use the Raw Socket protocol. For more information, refer to Section 5.4.5, “Configuring a Serial Port”.
2. Navigate to ***Serial Protocols*** » ***Configure Protocols*** » ***Configure Raw Socket*** » ***Configure Protocol***. The **Protocol** table appears.

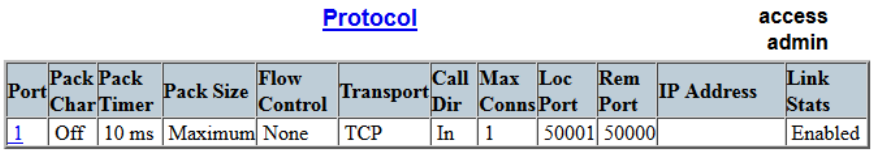


Figure 85: Protocol Table

3. Select a serial port. The **Protocol** form appears.

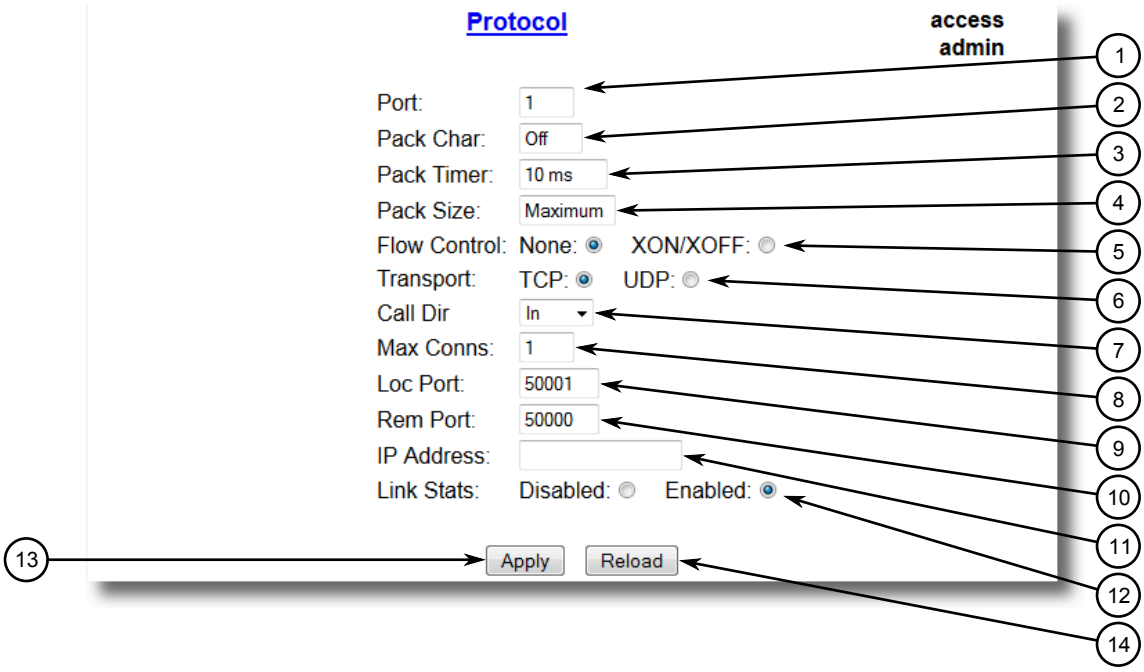


Figure 86: Protocol Form

1. Port Box **2.** Pack Char Box **3.** Pack Timer Box **4.** Pack Size Box **5.** Flow Control Options **6.** Transport Options **7.** Call Dir List **8.** Max Conns Box **9.** Loc Port Box **10.** Rem Port Box **11.** IP Address Box **12.** Link Stats Options **13.** Apply Button **14.** Reload Button

4. Configure the following parameter(s) as required:

Parameter	Description
Port	**Synopsis:** 1 to maximum port number

Parameter	Description
	Default: 1 The port number as seen on the front plate silkscreen of the switch.
Pack Char	**Synopsis:** 0 to 255 or { Off } **Default:** Off The character that can be used to force forwarding of accumulated data to the network. If a packetization character is not configured, accumulated data will be forwarded based upon the packetization timeout (Pack Timer) parameter.
Pack Timer	**Synopsis:** 3 to 1000 **Default:** 10 ms The delay from the last received character until when data is forwarded.
Pack Size	**Synopsis:** 64 to 1400 or { Maximum } **Default:** Maximum The maximum number of bytes received from the serial port to be forwarded.
Flow Control	**Synopsis:** { None, XON/XOFF } **Default:** None The Flowcontrol setting for serial port.
Transport	**Synopsis:** { TCP, UDP } **Default:** TCP The network transport used to transport protocol data over IP network.
Call Dir	**Synopsis:** { In, Out, Both } **Default:** In The Call direction for TCP Tranport. • Whether to accept an incoming connection or • to place an outgoing connection or • to place outgoing connection and wait for incomming (both directions).
Max Conns	**Synopsis:** 1 to 64 **Default:** 1 The maximum number of allowed incoming TCP connections (for configurations using TCP).
Loc Port	**Synopsis:** 1024 to 65535 **Default:** 50000 The local IP port to use when listening for an incoming connection or UDP data.
Rem Port	**Synopsis:** 1 to 65535 **Default:** 50000 The remote TCP port to use when placing an outgoing connection. Note that this parameter is applicable only to TCP connections. If the transport protocol is set to UDP, the remote port is configured using the "Remote Hosts" table.
IP Address	**Synopsis:** ###.###.###.### where ### ranges from 0 to 255 or { } For direction: 'Out' (client), the remote IP address to use when placing an outgoing TCP connection request. For direction: 'In' (server), the local interface IP address on which to listen for connection requests. An empty string implies the default: the IP address of the management interface. For direction: 'Both' (client or server), the remote IP address to use when placing an outgoing TCP connection request. The listening interface will be chosen by matching mask. Note that this parameter is applicable only to TCP connections. If the transport protocol is set to UDP, the remote port is configured using the "Remote Hosts" table.
Link Stats	**Synopsis:** { Disabled, Enabled } **Default:** Enabled

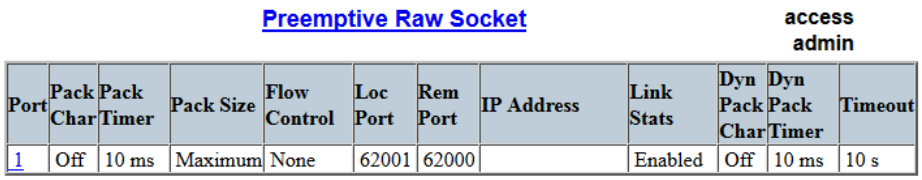
Parameter	Description
	Enables link statistics collection for the protocol.

5. Click **Apply**.
6. Add one or more remote hosts. For more information, refer to Section 5.4.16.2, “Adding a Remote Host”.

Section 5.4.7
Configuring the Preemptive Raw Socket Protocol

To configure the Preemptive Raw Socket protocol for a serial port, do the following:

1. Make sure the serial port is configured to use the Preemptive Raw Socket protocol. For more information, refer to Section 5.4.5, “Configuring a Serial Port”.
2. Navigate to ***Serial Protocols*** » ***Configure Protocols*** » ***Configure Preemptive Raw Socket***. The **Preemptive Raw Socket** table appears.



Preemptive Raw Socket

access
admin

Port	Pack Char	Pack Timer	Pack Size	Flow Control	Loc Port	Rem Port	IP Address	Link Stats	Dyn Pack Char	Dyn Pack Timer	Timeout
1	Off	10 ms	Maximum	None	62001	62000		Enabled	Off	10 ms	10 s

Figure 87: Preemptive Raw Socket Table

3. Select a serial port. The **Preemptive Raw Socket** form appears.

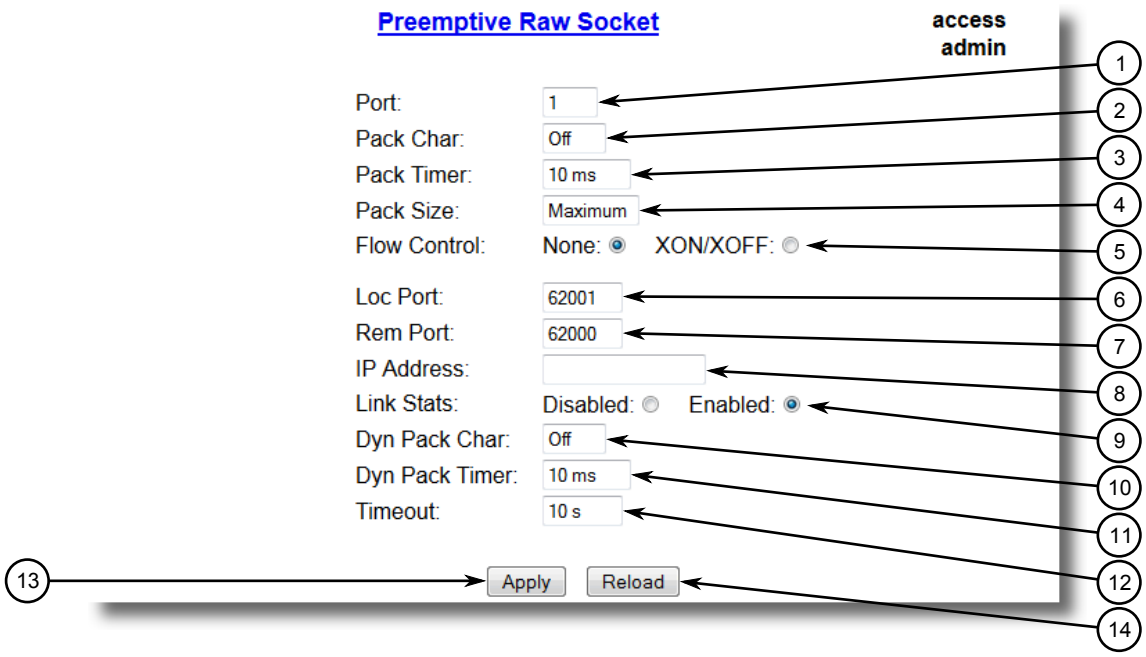


Figure 88: Preemptive Raw Socket Form

1. Port Box **2.** Pack Char Box **3.** Pack Timer Box **4.** Pack Size Box **5.** Flow Control Options **6.** Loc Port Box **7.** Rem Port Box **8.** IP Address Box **9.** Link Stats Options **10.** Dyn Pack Char Box **11.** Dyn Pack Timer Box **12.** Timeout Box **13.** Apply Button **14.** Reload Button

4. Configure the following parameter(s) as required:

Parameter	Description
Pack Size	**Synopsis:** 16 to 1400 or { Maximum } **Default:** Maximum The maximum number of bytes received from serial port to be forwarded.
Dyn Pack Char	**Synopsis:** 0 to 255 or { Off } **Default:** Off The character that can be used to force forwarding of accumulated data to the network for connection to dynamic master.If a packetization character is not configured, accumulated data will be forwarded based upon the packetization timeout parameter.
Loc Port	**Synopsis:** 1 to 65535 **Default:** 62001 The local IP port to use when listening for an incoming connection or UDP data.
Rem Port	**Synopsis:** 1 to 65535 **Default:** 62000 The remote TCP port to use when placing an outgoing connection.
Port	**Default:** 1 The port number as seen on the front plate silkscreen of the switch.
Pack Char	**Synopsis:** 0 to 255 or { Off } **Default:** Off

Parameter	Description
	The character that can be used to force forwarding of accumulated data to the network.If a packetization character is not configured, accumulated data will be forwarded based upon the packetization timeout parameter.
Pack Timer	**Synopsis:** 1 to 1000 ms **Default:** 10 ms The delay from the last received character until when data is forwarded.If parameter value is set to be less than 3 ms, there is not guaranty that it will be obeyed. It will be a minimum possible time in which device can react under certain data load.
Dyn Pack Timer	**Synopsis:** 1 to 1000 ms **Default:** 10 ms The delay from the last received character until when data is forwarded to the dynamic master.
Flow Control	**Synopsis:** { None, XON/XOFF } **Default:** None The Flowcontrol setting for serial port.
IP Address	**Synopsis:** ###.###.###.### where ### ranges from 0 to 255 or { <empty string> } The permanent master's IP address. Empty string represents management IP address of this device.
Link Stats	**Synopsis:** { Disabled, Enabled } **Default:** Enabled Enables links statistics collection for protocol.
Timeout	**Synopsis:** 10 to 3600 s **Default:** 10 s The time in seconds that is allowed to dynamic master to be idle before it's connection is closed. The protocol listens to the socket open to dynamic master, and if no data are received within this time, connection will be closed.

5. Click **Apply**.

Section 5.4.8

Configuring a TCP Modbus Server

To configure the TCP Modbus Server protocol for a serial port, do the following:

1. Make sure the serial port is configured to use the TCP Modbus Server protocol. For more information, refer to Section 5.4.5, “Configuring a Serial Port”.
2. Navigate to ***Serial Protocols*** » ***Configure Protocols*** » ***Configure Modbus Server***. The **Modbus Server** table appears.

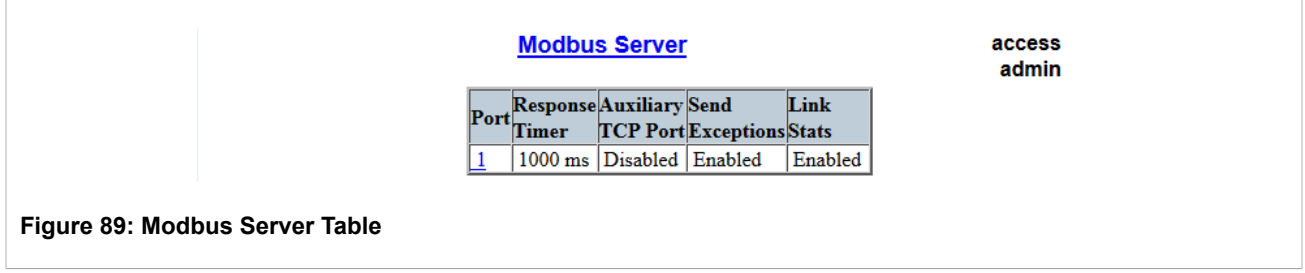


Figure 89: Modbus Server Table

3. Select a serial port. The **Modbus Server** form appears.

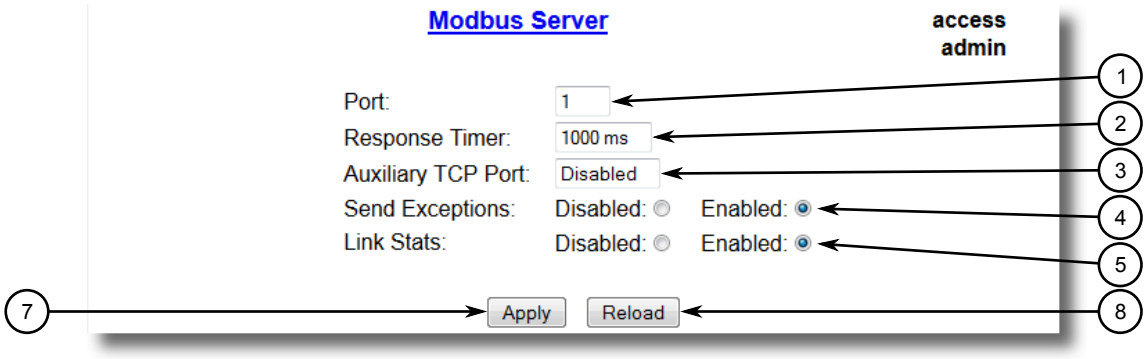


Figure 90: Modbus Server Form

1. Port Box **2.** Response Timer Box **3.** Auxiliary TCP Port Box **4.** Send Exceptions Options **5.** Link Stats Options **6.** Apply Button **7.** Reload Button

4. Configure the following parameter(s) as required:

Parameter	Description
Port	**Synopsis:** 1 to maximum port number **Default:** 1 The port number as seen on the front plate silkscreen of the switch.
Response Timer	**Synopsis:** 50 to 10000 **Default:** 1000 ms The maximum allowable time to wait for the RTU to start to respond.
Auxiliary TCP Port	**Synopsis:** 1024 to 65535 or { Disabled } **Default:** Disabled The TCP Modbus Server always listens on TCP port 502. It may be additionally configured to listen on this auxiliary port number, accepting calls on both.
Send Exceptions	**Synopsis:** { Disabled, Enabled } **Default:** Enabled This parameter enables/disables sending a TCP Modbus exception back to the master if a response has not been received from the RTU within expected time.
Link Stats	**Synopsis:** { Disabled, Enabled } **Default:** Enabled Enables link statistics collection for this protocol.

5. Click **Apply**.

Section 5.4.9

Configuring a TCP Modbus Client

To configure the TCP Modbus Client protocol for a serial port, do the following:

1. Make sure the serial port is configured to use the TCP Modbus Client protocol. For more information, refer to Section 5.4.5, “Configuring a Serial Port”.

2. Navigate to ***Serial Protocols*** » ***Configure Protocols*** » ***Configure Modbus Client***. The **Modbus Client** form appears.

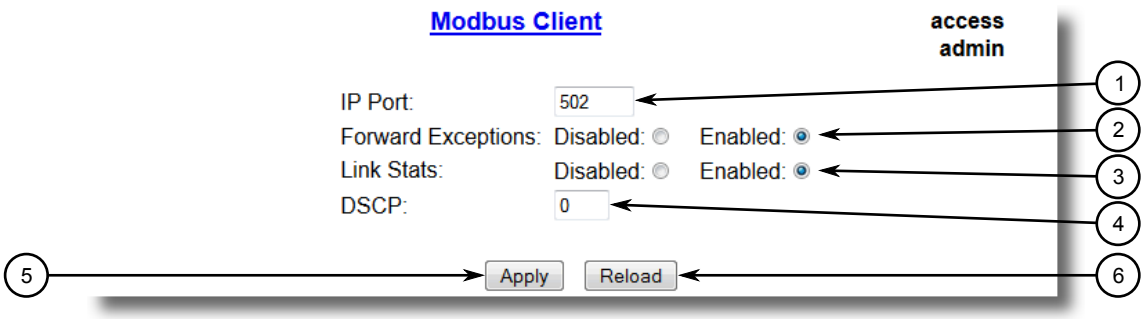


Figure 91: Modbus Client Form

1. IP Port Box **2.** Forward Exceptions Options **3.** Link Stats Options **4.** DSCP Box **5.** Apply Button **6.** Reload Button

3. Configure the following parameter(s) as required:

Parameter	Description
IP Port	**Synopsis:** 1 to 65535 **Default:** 502 The remote port number at which the Modbus protocol makes TCP connection requests.
Forward Exceptions	**Synopsis:** { Disabled, Enabled } **Default:** Enabled Enables forwarding exception messages to the Master as exception codes 10 (no path) or 11 (no response) When the Master polls for an unconfigured RTU or the remote Modbus Server receives a poll for an RTU which is not configured or is timing out, it returns an exception message. Disable this feature if your Master does not support exceptions but recognizes failure by time-out when waiting for response.
Link Stats	**Synopsis:** { Disabled, Enabled } **Default:** Enabled Enables link statistics collection for this protocol.
DSCP	**Synopsis:** 0 to 63 **Default:** 0 To set the DS byte in the IP header. DS byte setting is supported in the egress direction only.

4. Click **Apply**.

Section 5.4.10

Configuring the WIN and TIN Protocols

To configure the WIN or TIN protocols for a serial port, do the following:

1. Make sure the serial port is configured to use either the WIN or TIN protocol. For more information, refer to Section 5.4.5, “Configuring a Serial Port”.
2. Navigate to ***Serial Protocols*** » ***Configure Protocols*** » ***Configure WIN and TIN***. The **WIN and TIN** form appears.

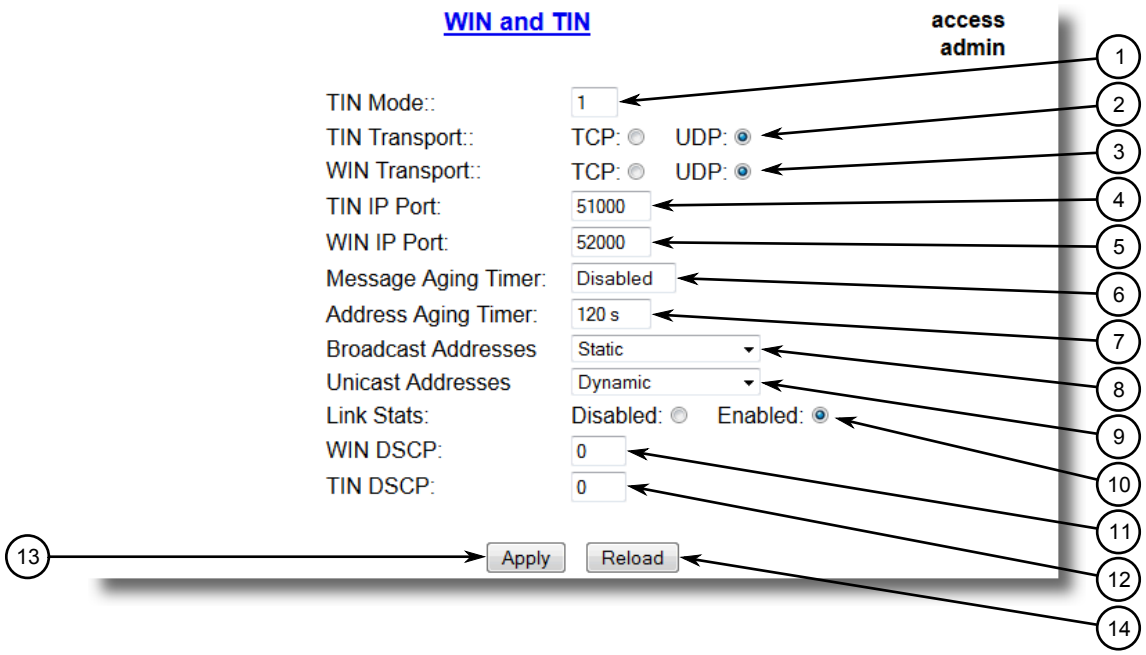


Figure 92: WIN and TIN Form

1. TIN Mode Box **2.** TIN Transport Options **3.** WIN Transport Options **4.** TIN IP Box **5.** WIN IP Box **6.** Messaging Aging Timer Box **7.** Address Aging Timer Box **8.** Broadcast Addresses List **9.** Unicast Addresses List **10.** Link Stats Options **11.** WIN DSCP Box **12.** TIN DSCP Box **13.** Apply Button **14.** Reload Button

3. Configure the following parameter(s) as required:

Parameter	Description
TIN Mode	**Synopsis:** 1 to 2 **Default:** 1 The TIN Protocol running mode.
TIN Transport	**Synopsis:** { TCP, UDP, Disabled } **Default:** UDP The network transport used to transport protocol data over an IP network.
WIN Transport	**Synopsis:** { TCP, UDP, Disabled } **Default:** UDP The network transport used to transport protocol data over an IP network.
TIN IP Port	**Synopsis:** 1024 to 65535 **Default:** 51000 The local port number on which the TIN protocol listens for connections or UDP datagrams.
WIN IP Port	**Synopsis:** 1024 to 65535 **Default:** 52000 The local port number on which the WIN protocol listens for connections or UDP datagrams.
Message Aging Timer	**Synopsis:** 1 to 3600 or { Disabled } **Default:** Disabled

Parameter	Description
	The Aging Time for TIN mode2 messages. It specifies how long a message should be stored in the internal table. When the feature is enabled, any TIN mode2 message received will be stored in an internal table which can be examined by using command 'SQL SELECT FROM ItcsTin2Dup'. If the same message is received within the time window specified by this parameter, the new message is considered duplicate, and thus discarded.
Address Aging Timer	**Synopsis:** 60 to 1000 **Default:** 300 s The time of communication inactivity after which a learned TIN address is removed from the device address table. Entries in the Link Statistics Table with the aged address will be kept until statistics are cleared.
Broadcast Addresses	**Synopsis:** { Static, Dynamic, StaticAndDynamic } **Default:** Static The device address table in which addresses will be found for broadcast messages.
Unicast Addresses	**Synopsis:** { Static, Dynamic, StaticAndDynamic } **Default:** Dynamic The device address table in which addresses will be found for unicast messages.
Link Stats	**Synopsis:** { Disabled, Enabled } **Default:** Enabled Enables link statistics collection for this protocol.
WIN DSCP	**Synopsis:** 0 to 63 **Default:** 0 To set the DS byte in the IP header. DS byte setting is supported in the egress direction only.
TIN DSCP	**Synopsis:** 0 to 63 **Default:** 0 To set the DS byte in the IP header. DS byte setting is supported in the egress direction only.

4. Click **Apply**.

Section 5.4.11
Configuring the MicroLok Protocol

To configure the MicroLok protocol for a serial port, do the following:

1. Make sure the serial port is configured to use the MicroLok protocol. For more information, refer to Section 5.4.5, “Configuring a Serial Port”.
2. Navigate to ***Serial Protocols*** » ***Configure Protocols*** » ***Configure MicroLok***. The **MicroLok** form appears.

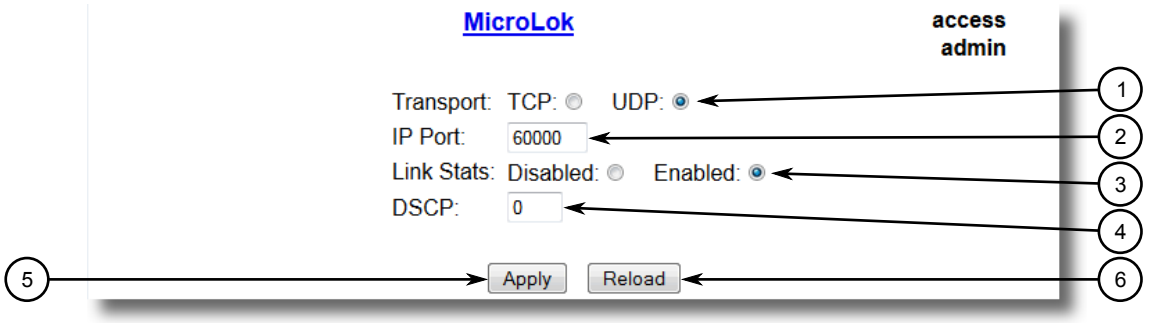


Figure 93: MicroLok Form

1. Transport Options **2.** IP Port Box **3.** Link Stats Options **4.** DSCP Box **5.** Apply Button **6.** Reload Button

3. Configure the following parameter(s) as required:

Parameter	Description
Transport	**Synopsis:** { TCP, UDP, Disabled } **Default:** UDP The network transport used to transport protocol data over an IP network.
IP Port	**Synopsis:** 1024 to 65535 **Default:** 60000 A local port number on which the MicroLok protocol listens for UDP datagrams or TCP connections.
Link Stats	**Synopsis:** { Disabled, Enabled } **Default:** Enabled Enables link statistics collection for this protocol.
DSCP	**Synopsis:** 0 to 63 **Default:** 0 To set the DS byte in the IP header. DS byte setting is supported in the egress direction only.

4. Click **Apply**.

Section 5.4.12

Configuring the DNP Protocol

To configure the DNP protocol for a serial port, do the following:

1. Make sure the serial port is configured to use the DNP protocol. For more information, refer to Section 5.4.5, "Configuring a Serial Port".
2. Navigate to ***Serial Protocols*** » ***Configure Protocols*** » ***Configure DNP Protocol*** » ***Configure DNP***. The **DNP** form appears.

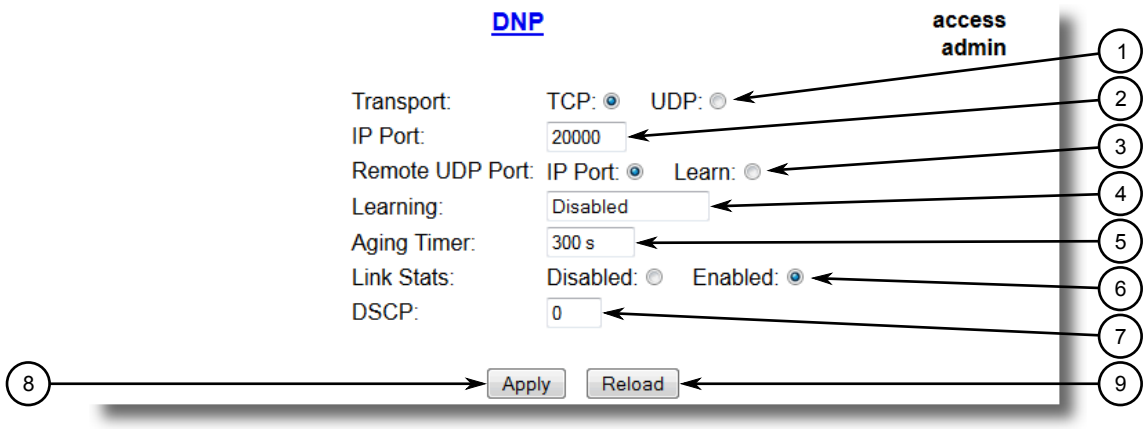


Figure 94: DNP Form

1. Transport Options **2.** IP Port Box **3.** Remote UDP Port Options **4.** Learning Box **5.** Aging Timer Box **6.** Link Stats Options **7.** DSCP Box **8.** Apply Button **9.** Reload Button

3. Configure the following parameter(s) as required:

Parameter	Description
Transport	**Synopsis:** { TCP, UDP, Disabled } **Default:** TCP The network transport used to transport protocol data over an IP network.
IP Port	**Synopsis:** 1024 to 65535 **Default:** 20000 A local port number on which the DNP protocol listens for UDP datagrams.
Remote UDP Port	**Synopsis:** { IP Port, Learn } **Default:** IP Port The IP port on which remote device listens to UDP datagrams. This port is either the same IP port that devices in all networks listen to, or can be learned from the UDP datagram.
Learning	**Synopsis:** ###.###.###.### where ### ranges from 0 to 255 or { Disabled } **Default:** Disabled Enable or disable address learning. Learning can be disabled or enabled on a management IP interface (empty string), or enabled on the interface with a specific IP address. If learning is enabled and the remote address is not known, a UDP broadcast message will be sent and source addresses will be learned on devices that run the DNP protocol. If the local address is not known, a message will be sent to all serial ports running the DNP protocol. Local addresses will be learned from local responses. If the TCP transport is configured, a connection will be established to the devices with the corresponding IP address.

4. Click **Apply**.

Section 5.4.13

Configuring the DNP Over Raw Socket Protocol

To configure the DNP Over Raw Socket protocol for a serial port, do the following:

1. Make sure the serial port is configured to use the DNP Over Raw Socket protocol. For more information, refer to Section 5.4.5, “Configuring a Serial Port”.
2. Navigate to ***Serial Protocols*** » ***Configure Protocols*** » ***Configure DNP Protocol*** » ***Configure DNP over RawSocket***. The **DNP over RawSocket** table appears.

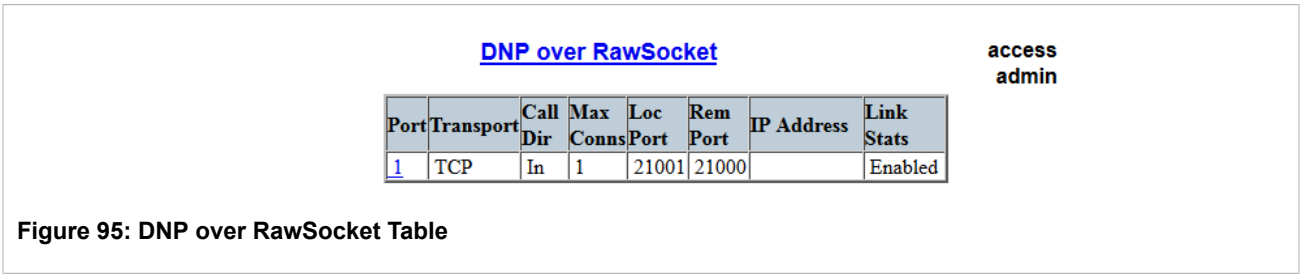


Figure 95: DNP over RawSocket Table

3. Select a serial port. The **DNP over RawSocket** form appears.

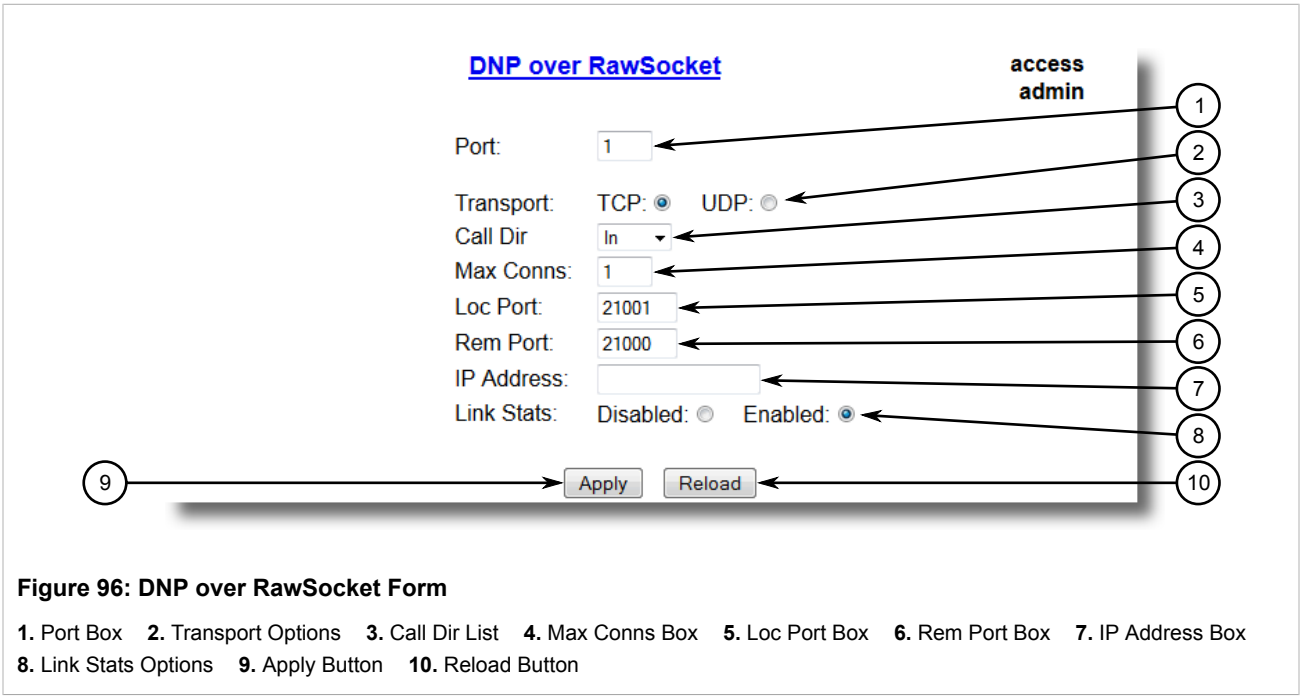


Figure 96: DNP over RawSocket Form

1. Port Box **2.** Transport Options **3.** Call Dir List **4.** Max Conns Box **5.** Loc Port Box **6.** Rem Port Box **7.** IP Address Box **8.** Link Stats Options **9.** Apply Button **10.** Reload Button

4. Configure the following parameter(s) as required:

Parameter	Description
Port	**Synopsis:** 1 to 4 **Default:** 1 The port number as seen on the front plate silkscreen on the switch.
Transport	**Synopsis:** { TCP, UDP } **Default:** TCP The network transport used to transport protocol data over the IP network.
Call Dir	**Synopsis:** { In, Out, Both }

Parameter	Description
	Default: In The Call direction for TCP Tranport. • In: accepts an incoming connection. • Out: places an outgoing connection • Both: places an outgoing connection and waits for as incoming connection (both directions).
Max Conns	**Synopsis:** 1 to 64 **Default:** 1 The maximum number of allowed incoming TCP connections.
Loc Port	**Synopsis:** 1 to 65535 **Default:** 21001 The local IP port to use when listening for an incoming connection or UDP data.
Rem Port	**Synopsis:** 1 to 65535 **Default:** 21000 The remote TCP port to use when placing an outgoing connection.
IP Address	**Synopsis:** ###.###.###.### (where ### ranges from 0 to 255) | { <empty string> } **Default:** <empty string> Defines the IP address based on the following: • For outgoing TCP connection (client), this is the remote IP address to communicate with. • For incoming TCP connection (server), this is the local interface IP address to listen to for the local port for connection request. If an empty string is configured, the IP address of the management interface is used. • When both outgoing and incoming connections are enabled (client or server), this is remote IP address to use to place an outgoing TCP connection request or from which to accept calls • For UDP transport, this is the IP address of the interface to listen to for UDP datagrams.
Link Stats	**Synopsis:** { Disabled, Enabled } **Default:** Enabled Enables links statistics collection for the protocol.

5. Click **Apply**.

Section 5.4.14
Configuring the Mirrored Bits Protocol

To configure the Mirrored Bits protocol for a serial port, do the following:

1. Make sure the serial port is configured to use the Mirrored Bits protocol. For more information, refer to Section 5.4.5, “Configuring a Serial Port”.
2. Navigate to ***Serial Protocols*** » ***Configure Protocols*** » ***Configure Mirrored Bits***. The **Mirrored Bits** table appears.

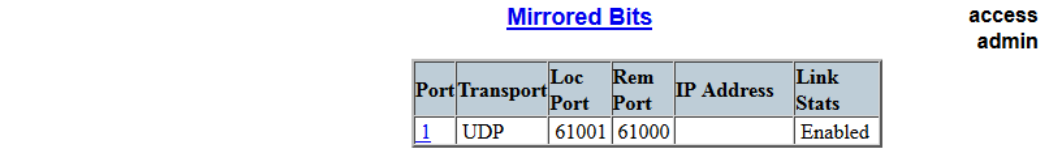


Figure 97: Mirrored Bits Table

3. Select a serial port. The **Mirrored Bits** form appears.

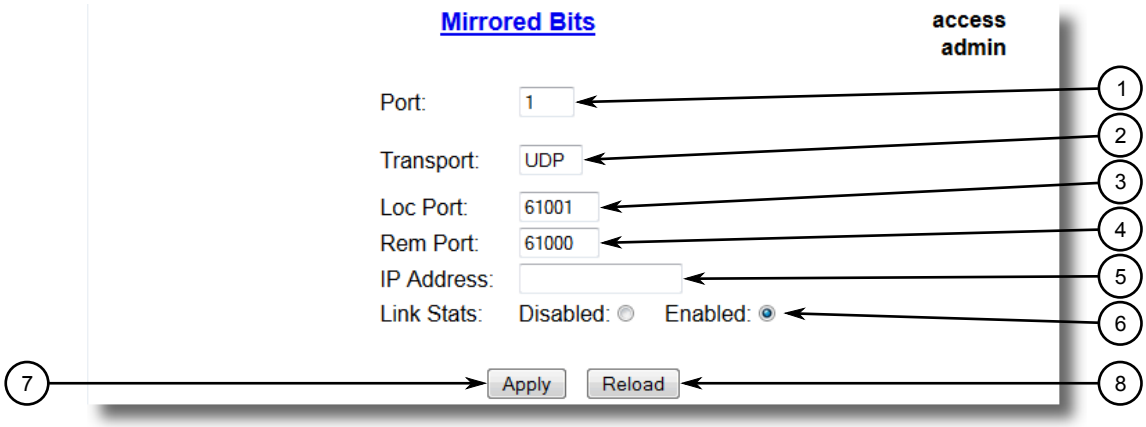


Figure 98: Mirrored Bits Form

1. Port Box **2.** Transport Box **3.** Loc Port Box **4.** Rem Port Box **5.** IP Address Box **6.** Link Stats Options **7.** Apply Button **8.** Reload Button

4. Configure the following parameter(s) as required:

Parameter	Description
Port	**Synopsis:** 1 to 4 **Default:** 1 The port number as seen on the front plate silkscreen of the switch.
Transport	**Synopsis:** { TCP, UDP } **Default:** UDP The network transport used to transport Mirrored Bits protocol data over an IP network.
Loc Port	**Synopsis:** 1 to 65535 **Default:** 61001 The local IP port to use when listening for an incoming connection or UDP data.
Rem Port	**Synopsis:** 1 to 65535 **Default:** 61000 The remote TCP port to use when placing an outgoing connection.
IP Address	**Synopsis:** ###.###.###.### where ### ranges from 0 to 255 or { <EMPTY STRING> } Default: For an outgoing TCP connection (client) and UDP transport, this is the remote IP address to communicate with.

Parameter	Description
	For an incoming TCP connection (server), the local interface IP address on which to listen for connection requests. An empty string implies the default: the IP address of the management interface. When both outgoing and incoming connections are enabled (client or server), this is the remote IP address to which to place an outgoing TCP connection request or from which to accept an incoming request.
Link Stats	**Synopsis:** { Disabled, Enabled } **Default:** Enabled Enables link statistics collection for this protocol.

5. Click **Apply**.

Section 5.4.15

Configuring the Telnet Com Port Protocol

To configure the Telnet Com Port protocol for a serial port, do the following:

1. Make sure the serial port is configured to use the Telnet Com Port protocol. For more information, refer to Section 5.4.5, “Configuring a Serial Port”.
2. Navigate to ***Serial Protocols » Configure Protocols » Configure Telnet Com Port***. The **Telnet Com Port** table appears.

Telnet Com Port

access admin

Port	Pack Char	Pack Timer	Pack Size	Flow Control	Call Dir	Loc Port	Rem Port	IP Address	Link Stats
1	Off	10 ms	Maximum	None	In	50001	50000		Enabled

Figure 99: Telnet Com Port Table

3. Select a serial port. The **Telnet Com Port** form appears.

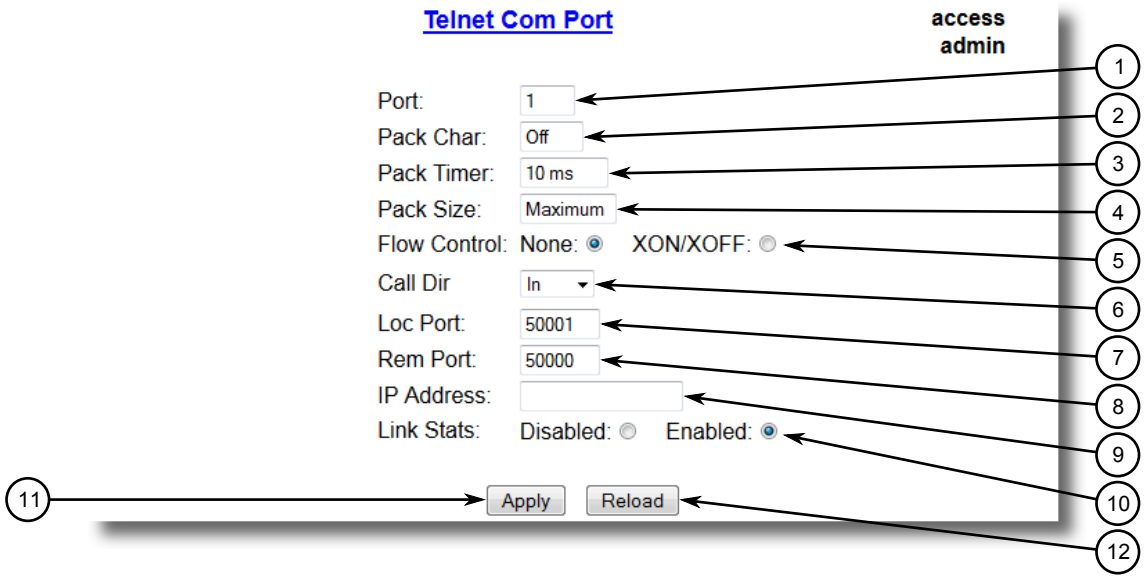


Figure 100: Telnet Com Port Form

1. Port Box **2.** Pack Char Box **3.** Pack Timer Box **4.** Pack Size Box **5.** Flow Control Options **6.** Call Dir List **7.** Loc Port Box **8.** Rem Port Box **9.** IP Address Box **10.** Link Stats Options **11.** Apply Button **12.** Reload Button

4. Configure the following parameter(s) as required:

Parameter	Description
Port	**Synopsis:** 1 to maximum port number **Default:** 1 The serial port number as seen on the front plate silkscreen of the RMC30.
Pack Char	**Synopsis:** 0 to 255 or { Off } **Default:** Off The character that will be used to force the forwarding of buffered data to the network. If a packetization character is not configured, buffered data will be forwarded based upon the packetization timeout (Pack Timer) parameter.
Pack Timer	**Synopsis:** 1 to 1000 **Default:** 10 ms The delay from the last received character until when data is forwarded. If parameter value is set to be less than 3 ms, there is not guaranty that it will be obeyed. It will be a minimum possible time in which device can react under certain data load.
Pack Size	**Synopsis:** 16 to 1400 or { Maximum } **Default:** Maximum The maximum number of bytes received from serial port to be forwarded.
Flow Control	**Synopsis:** { None, XON/XOFF } **Default:** None The Flowcontrol setting for serial port.
Call Dir	**Synopsis:** { In, Out, Both } **Default:** In The Call direction for TCP Transport. • Whether to accept an incoming connection or

Parameter	Description
	• to place an outgoing connection or • to place outgoing connection and wait for incoming (both directions).
Loc Port	**Synopsis:** 1024 to 65535 **Default:** 50000 The local IP port to use when listening for an incoming connection.
Rem Port	**Synopsis:** 1 to 65535 **Default:** 50000 The remote TCP port to use when placing an outgoing connection. This parameter is applicable only to TCP transport.
IP Address	**Synopsis:** ###.###.###.### where ### ranges from 0 to 255 or { } **Default:** For direction 'OUT' (client), remote IP address to use when placing an outgoing TCP connection request. For direction 'IN' (server), local interface IP address to listen to the local port for connection request. Empty string can be used for IP address of management interface. For direction 'BOTH' (client or server), remote IP address to use when placing an outgoing TCP connection requestListening interface will be chosen by matching mask. This parameter is applicable only to TCP connections. If the transport protocol is set to UDP, the remote port is configured using the "Remote Hosts" table.
Link Stats	**Synopsis:** { Disabled, Enabled } **Default:** Enabled Enables links statistics collection for this protocol.

5. Click **Apply**.

Section 5.4.16

Managing Raw Socket Remote Hosts

The following sections describe how to configure and manage remote hosts:

- Section 5.4.16.1, “Viewing a List of Remote Hosts”
- Section 5.4.16.2, “Adding a Remote Host”
- Section 5.4.16.3, “Deleting a Remote Host”

Section 5.4.16.1

Viewing a List of Remote Hosts

To view a list of remote hosts configured for the Raw socket protocol, navigate to ***Serial Protocols*** » ***Configure Protocols*** » ***Configure Raw Socket*** » ***Configure Remote Hosts***. The **Remote** table appears.

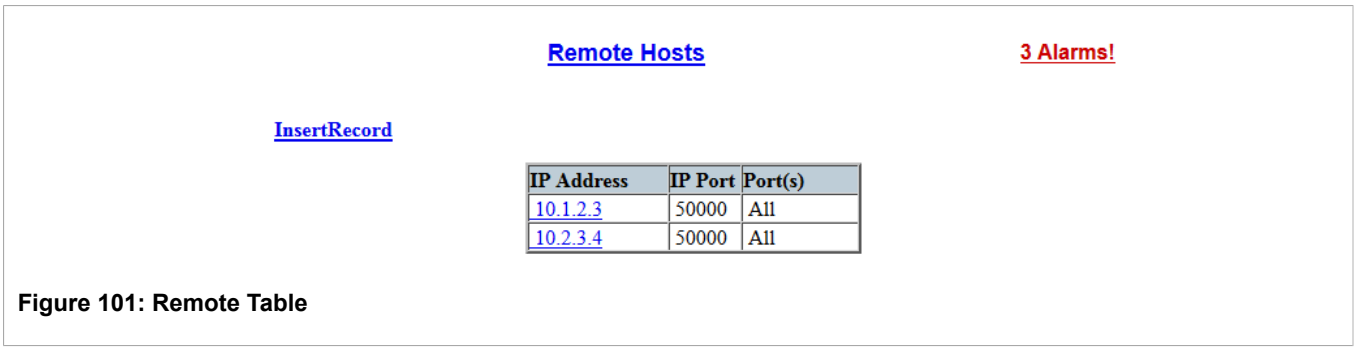


Figure 101: Remote Table

If remote hosts have not been configured, add hosts as needed. For more information, refer to Section 5.4.16.2, "Adding a Remote Host".

Section 5.4.16.2

Adding a Remote Host

To add a remote host for the Raw socket protocol, do the following:

1. Navigate to ***Serial Protocols*** » ***Configure Protocols*** » ***Configure Raw Socket*** » ***Configure Remote Hosts***. The **Remote Hosts** table appears.

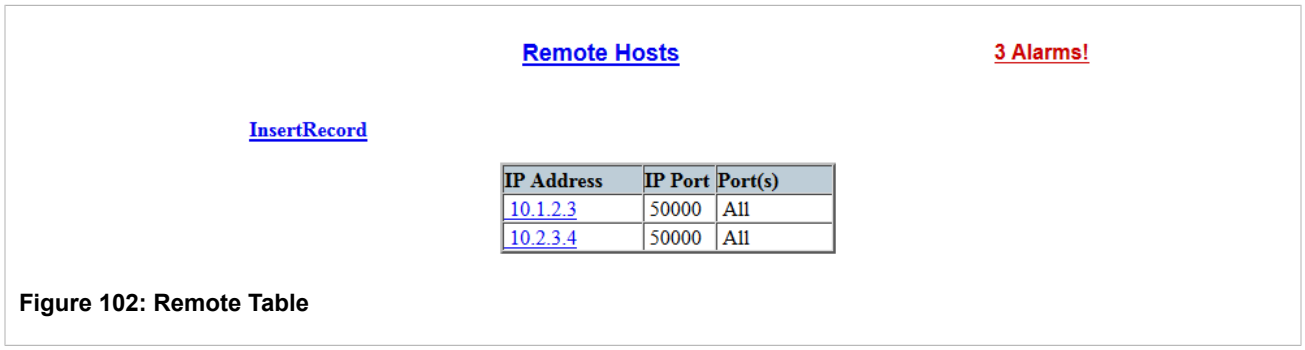


Figure 102: Remote Table

2. Click **InsertRecord**. The **Remote Hosts** form appears.

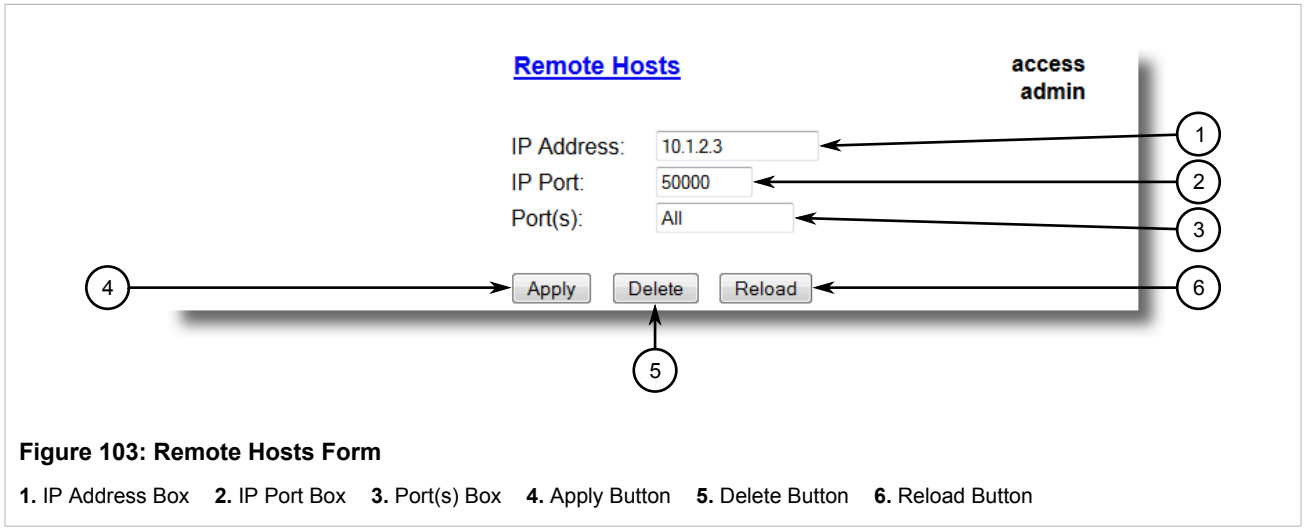


Figure 103: Remote Hosts Form

1. IP Address Box **2.** IP Port Box **3.** Port(s) Box **4.** Apply Button **5.** Delete Button **6.** Reload Button

3. Configure the following parameter(s) as required:

Parameter	Description
IP Address	**Synopsis:** ###.###.###.### where ### ranges from 0 to 255 **Default:** The IP address of the remote host.
IP Port	**Synopsis:** 1 to 65535 or { Unknown } **Default:** 50000 The IP port that remote host listens to. If this is zero (Unknown), the unit only receives from the remote host but does not transmit to it.
Port(s)	**Synopsis:** Any combination of numbers valid for this parameter **Default:** All The local serial ports that the remote host is allowed to communicate with.

4. Click **Apply**.

Section 5.4.16.3
Deleting a Remote Host

To delete a remote host used by the Raw socket protocol, do the following:

1. Navigate to ***Serial Protocols*** » ***Configure Protocols*** » ***Configure Raw Socket*** » ***Configure Remote Hosts***. The **Remote** table appears.

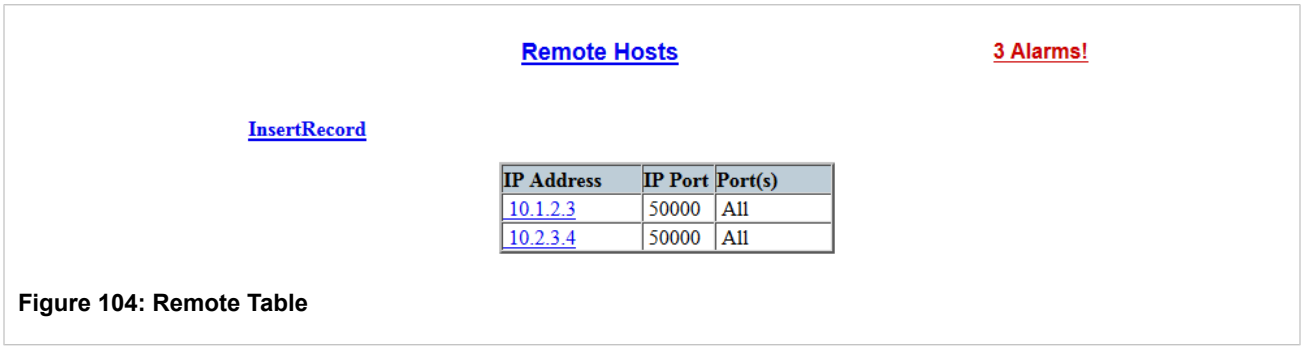


Figure 104: Remote Table

2. Select the remote host from the table. The **Remote** form appears.

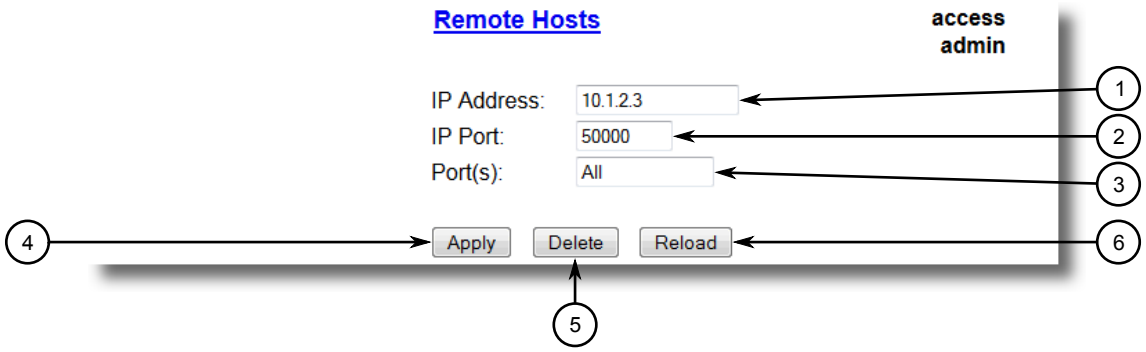


Figure 105: Remote Form

1. IP Address Box **2.** IP Port Box **3.** Port(s) Box **4.** Apply Button **5.** Delete Button **6.** Reload Button

3. Click **Delete**.

Section 5.4.17

Managing Device Addresses

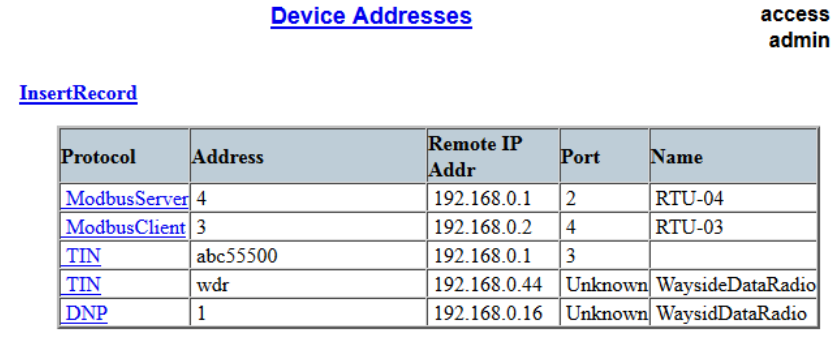
The following sections describe how to configure and manage device addresses:

- Section 5.4.17.1, “Viewing a List of Device Addresses”
- Section 5.4.17.2, “Adding a Device Address”
- Section 5.4.17.3, “Deleting a Device Address”

Section 5.4.17.1

Viewing a List of Device Addresses

To view a list of device addresses configured on the device, navigate to ***Serial Protocols » Configure Device Address Table***. The **Device Address Table** table appears.



Protocol	Address	Remote IP Addr	Port	Name
ModbusServer	4	192.168.0.1	2	RTU-04
ModbusClient	3	192.168.0.2	4	RTU-03
TIN	abc55500	192.168.0.1	3	
TIN	wdr	192.168.0.44	Unknown	WaysideDataRadio
DNP	1	192.168.0.16	Unknown	WaysidDataRadio

Figure 106: Device Address Table Table

If device addresses have not been configured, add addresses as needed. For more information, refer to Section 5.4.17.2, “Adding a Device Address”.

Section 5.4.17.2
Adding a Device Address

To add a device address, do the following:

1. Navigate to ***Serial Protocols*** » ***Configure Device Addresses***. The **Device Address Table** table appears.

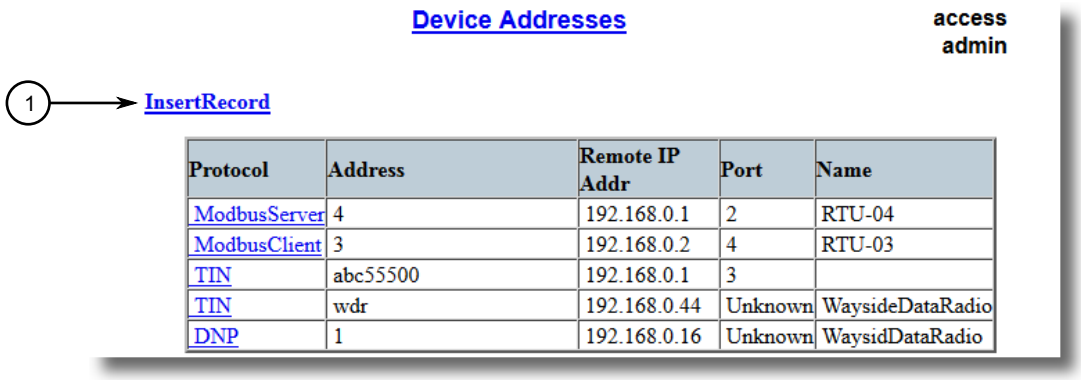


Figure 107: Device Address Table Table

1. InsertRecord

2. Click **InsertRecord**. The **Device Address Table** form appears.

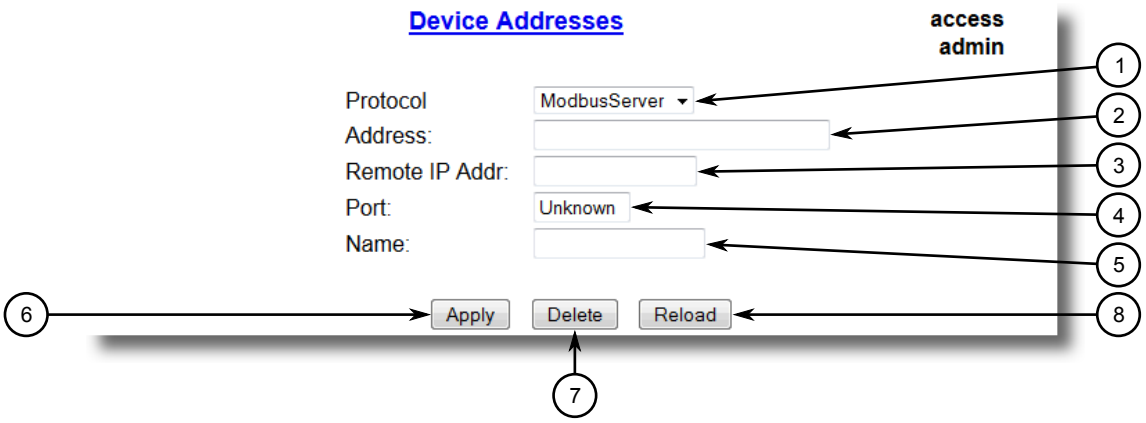


Figure 108: Device Address Table Form

1. Protocol List **2.** Address Box **3.** Remote IP Address Box **4.** Port Box **5.** Name Box **6.** Apply Button **7.** Delete Button **8.** Reload Button

3. Configure the following parameter(s) as required:

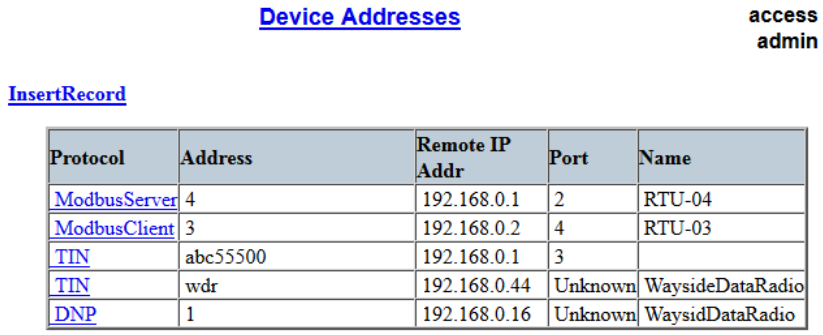
Parameter	Description
Protocol	**Synopsis:** { ModbusServer, ModbusClient, DNP, WIN, TIN, MicroLok } **Default:** ModbusServer The serial protocol supported on this serial port.
Address	**Synopsis:** Any 31 characters Default: The complete address of a device, which might be either local to the RUGGEDCOM device or remote. A local address is one associated with a device connected to a serial port on this device. The corresponding serial port must be configured to match this address specification. A remote address is the address of a device connected to a serial port on a remote host over an IP network. In this case, "Remote Ip Addr" must also be configured. The format and range of this address field is determined by the protocol: • Modbus: 1 to 244 • MicroLok: 1 to 65535, or 8 to hexadecimal digits ‘1’ to ‘a’ • DNP 3.0: 1 to 65520 • WIN: 6 bits address (0 to 63) • TIN: String 'wdr' for wayside data radio (TIN mode 2), or a 32 bit address (8 digits, expressed in hexadecimal digits '0' through 'f'). An all-zero address is not allowed.
Remote IP Addr	**Synopsis:** ###.###.###.### where ### ranges from 0 to 255 Default: The IP address of a remote host where a device with a configured remote address is connected.
Port	**Synopsis:** 1 to maximum port number or {Unknown} **Default:** Unknown The serial port to which a device is attached. If the device with this address is attached to the serial port of a remote host, the value of this parameter is 'Unknown'.
Name	**Synopsis:** Any 16 characters Default: The addressed device name.

4. Click **Apply**.

Section 5.4.17.3
Deleting a Device Address

To delete a device address, do the following:

1. Navigate to ***Serial Protocols » Configure Device Address Table***. The **Device Address Table** table appears.



Protocol	Address	Remote IP Addr	Port	Name
ModbusServer	4	192.168.0.1	2	RTU-04
ModbusClient	3	192.168.0.2	4	RTU-03
TIN	abc55500	192.168.0.1	3	
TIN	wdr	192.168.0.44	Unknown	WaysideDataRadio
DNP	1	192.168.0.16	Unknown	WaysidDataRadio

Figure 109: Device Address Table Table

2. Select the device address from the table. The **Device Address Table** form appears.

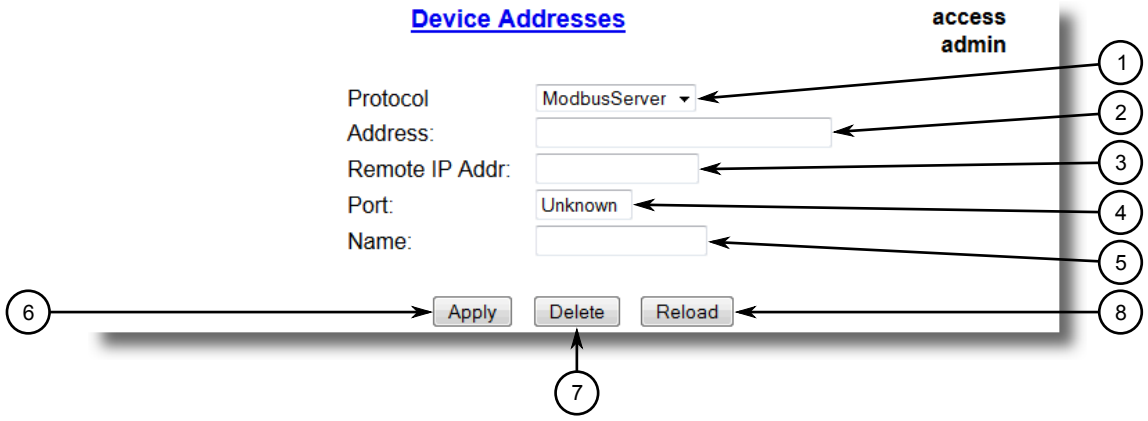


Figure 110: Device Address Table Form

1. Protocol List **2.** Address Box **3.** Remote IP Address Box **4.** Port Box **5.** Name Box **6.** Apply Button **7.** Delete Button **8.** Reload Button

3. Click **Delete**.

Section 5.4.18

Viewing the TIN Dynamic Address Table

To view the device addresses learned dynamically by the TIN protocol from remote locations, navigate to ***Serial Protocols » View TIN Dynamic Address Table***. The **TIN Dynamic Address Table** table appears.

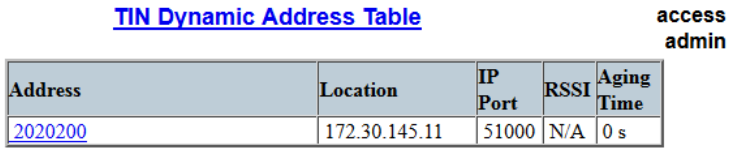


Figure 111: TIN Dynamic Address Table

This table displays the following information:

Parameter	Description
Address	**Synopsis:** Any 31 characters The remote device address.
Location	**Synopsis:** ###.###.###.### where ### ranges from 0 to 255 The IP Address of the remote host.
IP Port	**Synopsis:** 1 to 65535 The remote port number through which remote device sent a UDP datagram or TCP connection is established
RSSI	**Synopsis:** -128 to 0 or { N/A } The signal strength indicator received from wayside data radio. N/A for TIN Mode 1.
Aging Time	**Synopsis:** 0 to 1000 s The amount of time since the last packet arrived from the device. Once this time exceeds the Aging Timer setting for protocol, the device will be removed from the table. This value is updated every 10 seconds.

Section 5.4.19

Viewing Statistics for Serial Protocol Links

To view statistics for serial protocol links, navigate to ***Serial Protocols » View Links Statistics***. The **Links Statistics** table appears.

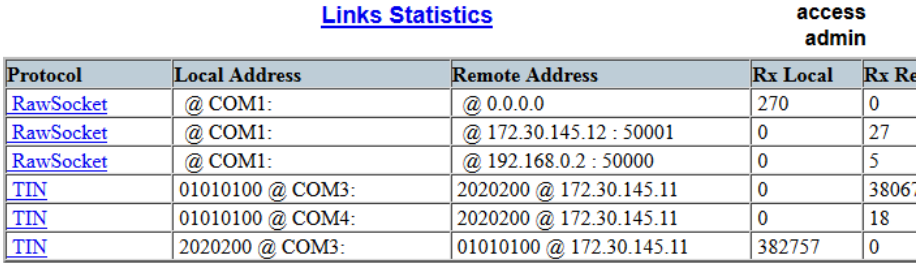


Figure 112: Links Statistics Table

This table displays the following information:

Parameter	Description
Protocol	**Synopsis:** { None, RawSocket, ModbusServer, ModbusClient, DNP, DNPRS, WIN, TIN, MicroLok, MirroredBits, PreemptRawSocket, TelnetComPort } The serial protocol supported by devices that create this link.
Local Address	**Synopsis:** Any 27 characters The address of the device connected to the serial port on this device.
Remote Address	**Synopsis:** Any 35 characters The address of the device connected to the remote host's serial port.
Rx Local	**Synopsis:** 0 to 4294967295 The number of packets received from the local address that were forwarded to the remote side.
Rx Remote	**Synopsis:** 0 to 4294967295 The number of packets received from the local address that were forwarded to the local serial port.
Erroneous	**Synopsis:** 0 to 4294967295 The number of erroneous packets received from the remote address.

Section 5.4.20

Viewing Statistics for Serial Protocol Connections

To view statistics for serial protocol connections, navigate to ***Serial Protocols » View Connection Statistics***. The **Connection Statistics** table appears.

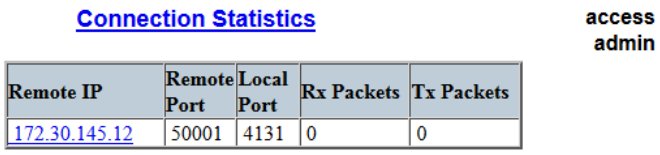


Figure 113: Connection Statistics Table

This table displays the following information:

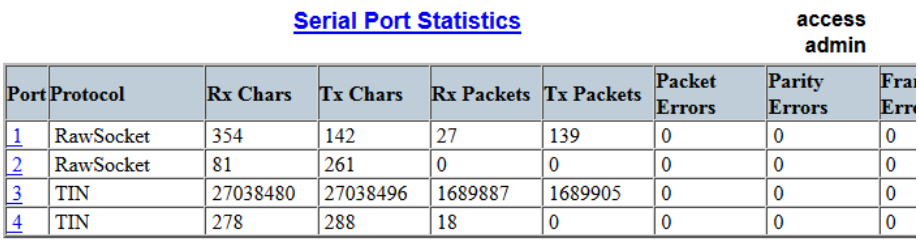
Parameter	Description
Remote IP	**Synopsis:** ###.###.###.### where ### ranges from 0 to 255 The remote IP address of the connection.
Remote Port	**Synopsis:** 0 to 65535 The remote port number of the connection.
Local Port	**Synopsis:** 0 to 65535 The local port number of the connection.
Rx Packets	**Synopsis:** 0 to 4294967295 The number of received packets on the connection.
Tx Packets	**Synopsis:** 0 to 4294967295

Parameter	Description
	The number of packets transmitted on the connection.

Section 5.4.21

Viewing Serial Port Statistics

To view statistics for serial ports, navigate to ***Serial Protocols » View Serial Port Statistics***. The **Serial Port Statistics** table appears.



Serial Port Statistics

access admin

Port	Protocol	Rx Chars	Tx Chars	Rx Packets	Tx Packets	Packet Errors	Parity Errors	Fra Err
1	RawSocket	354	142	27	139	0	0	0
2	RawSocket	81	261	0	0	0	0	0
3	TIN	27038480	27038496	1689887	1689905	0	0	0
4	TIN	278	288	18	0	0	0	0

Figure 114: Serial Port Statistics Table

This table displays the following information:

Parameter	Description
Port	**Synopsis:** 1 to maximum port number The port number as seen on the front plate silkscreen of the switch.
Protocol	**Synopsis:** Any 15 characters The serial protocol supported on this serial port.
Rx Chars	**Synopsis:** 0 to 4294967295 The number of received characters.
Tx Chars	**Synopsis:** 0 to 4294967295 The number of transmitted characters.
Rx Packets	**Synopsis:** 0 to 4294967295 The number of received packets.
Tx Packets	**Synopsis:** 0 to 4294967295 The number of transmitted packets.
Packet Errors	**Synopsis:** 0 to 4294967295 The number of packets received from this port and discarded (error in protocol, CRC or routing information not found).
Parity Errors	**Synopsis:** 0 to 4294967295 The number of Parity Errors.
Framing Errors	**Synopsis:** 0 to 4294967295 The number of Framing Errors.
Overrun Errors	**Synopsis:** 0 to 4294967295

Parameter	Description
	The number of Overrun Errors.

Section 5.4.22
Clearing Statistics for Specific Serial Ports

To clear the statistics collected for one or more serial ports, do the following:

1. Navigate to ***Serial Protocols*** » ***Clear Serial Port Statistics***. The **Clear Serial Port Statistics** form appears.

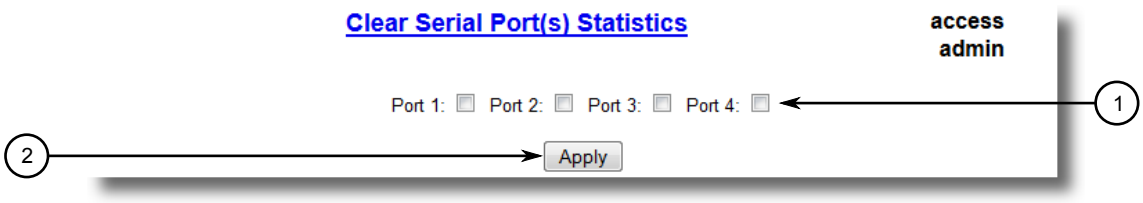


Figure 115: Clear Serial Port Statistics Form

1. Port Check Boxes **2.** Confirm Button

2. Select one or more serial ports.
3. Click **Confirm**.

Section 5.4.23
Resetting Serial Ports

To reset a specific serial port(s), do the following:

1. Navigate to ***Serial Protocols*** » ***Reset Serial Port(s)***. The **Reset Serial Port(s)** form appears.

Figure 116: Reset Serial Port(s) Form

1. Ports **2.** Apply Button

2. Select one or more serial ports to reset.
3. Click **Apply**. The selected serial ports are reset.

6 Troubleshooting

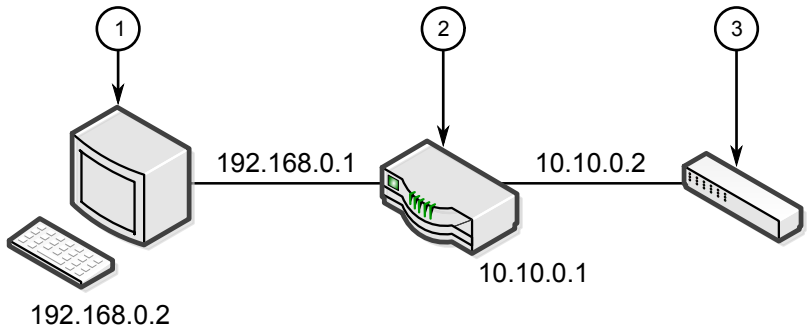
This chapter describes troubleshooting steps for common issues that may be encountered when using ROS or designing a network. It describes the following tasks:

IMPORTANT!
For further assistance, contact a Customer Service representative.

- Section 6.1, “General”

Section 6.1
General

The following describes common problems.

Problem	Solution
The switch is not responding to ping attempts, even though the IP address and gateway have been configured. The switch is receiving the ping because the LEDs are flashing and the device statistics are logging the pings. What is going on?	Is the switch being pinged through a router? If so, the switch gateway address must be configured as well. The following figure illustrates the problem.  **Figure 117: Using a Router As a Gateway** **1.** Work Station **2.** Router **3.** Switch The router is configured with the appropriate IP subnets and will forward the ping from the workstation to the switch. When the switch responds, however, it will not know which of its interfaces to use in order to reach the workstation and will drop the response. Programming a gateway of 10.0.0.1 will cause the switch to forward unresolvable frames to the router. This problem will also occur if the gateway address is not configured and the switch tries to raise an SNMP trap to a host that is not on the local subnet.